拔尖班数论与代数基础讲义

张起帆

2013年，2-6月

Contents

*引论

本课程是以前的两门课初等数论和近世代数基础的合并。近几年的基础数学专业有系列课程初等数论、近世代数基础和抽象代数，分别是2学分、2学分和4学分。对拔尖班曾尝试将后两个课合并，缺点是一学期6学分让学生负担太重。这次的尝试不仅让学分分配更合理，还有以下原因：

数论是研究整数和有理数这些最具体的数学对象的学科，近世代数是研究群、环、域等抽象结构的学科。数论中会出现自然的群、环、域的例子，使代数概念的出现更加自然，代数理论使数论方法更加系统和易接受。

自己总结整数（不一定是正整数）的基本知识，比如整除，最大公约数，最小公倍数，素数、合数和互素等概念。一般地，对整数a,b，我们用(a,b)或$g.c.d.(a,b)$表示最大公约数；用$[a,b]$或$l.c.m.[a,b]$表示最小公倍数；一般情形下，p都代表素数。

唯一分解定理

第一周 唯一分解定理及简单应用

1 带余除法

对任意整数a,b，$b>0$，存在唯一整数q,r满足

$$a=bq+r, 0\le r<b$$

这是小学生都知道的事实，但却是至关重要的。它可以给出求最大公约数的Euclid算法：设a,b为正整数且$a>b$, 则可不断做带余除法

$$a=bq_1+b_1$$

$$b=b_1q_2+b_2$$

$$\cdots$$

$$b_n=b_{n+1}q_{n+2}+0$$

则$b_{n+1}=(a,b)$ 因为

$$(a,b)=(a-b,b)=(a-2b,b)=\cdots=(b_1,b)=(b-b_1,b_1)=\cdots=(b_2,b_1)=\cdots=(b_{n+1},b_n)=b_{n+1}$$

从上述算法得出如下结论，由于很重要，作为定理

定理1.1. 对任意整数a,b，存在整数u,v，满足$(a,b)=au+bv$

有了这个定理我们容易得到如下结论：

引理1.2. 对整数a,b,c，若$(a,b)=1$，则

$$a|bc\Longrightarrow a|c$$

证明：因为$(a,b)=1$，故存在整数u,v，满足

$$1=au+bv$$

即

$$c=acu+bcv$$

由于两项都是a的倍数，故$a|c$。

推论：对素数p有

$$p|ab\Longrightarrow p|a\text{或}p|b$$

2 同余语言的引进

对整数a,b,m，称a模m同余于b，记为$a\equiv b\pmod m$是指a和b用m除的余数相同，换句话说$m|a-b$。例如

$$17\equiv 10\equiv 3\pmod 7$$

同余思想简单来说就是在带余除法中忽略商，只关心余数，在某些场合，这就突出了重点，看问题更清晰，现重新叙述前面的推理:

Eulcid算法：对整数$a>b>0$，一定有

$a\equiv b_1\pmod b$，（对某一整数b_1，$0\le b_1<b$）

$b\equiv b_2\pmod{b_1}$，（对某一整数b_2，$0\le b_2<b_1$）

$\cdots$

$b_{n-1}\equiv b_{n+1}=0\pmod{b_n}$

$(a,b)=b_n$

同样地，前面的定理和引理以及证明都可以用同余语言重新叙述：

定理1.1.1

对任意整数a,b，存在整数v使$bv\equiv(a,b)\pmod a$，特别地，若$(a,b)=1$，则有$bv\equiv 1\pmod a$

引理的证明：因$(a,b)=1$，故存在v满足$bv\equiv 1\pmod a$，在$bc\equiv 0\pmod a$中两边同乘v有$c\equiv bvc\equiv 0\pmod a$

注：有了同余语言，立刻应想到（省略证明）如下性质:

(1) 模某个m的同余关系是等价关系；

(2) $a\equiv b\pmod m, c\equiv d\pmod m\Longrightarrow a+c\equiv b+d\pmod m$;

(3) $a\equiv b\pmod m, c\equiv d\pmod m\Longrightarrow ac\equiv bd\pmod m$;

3 唯一分解定理及证明

定理3.1. 任意大于*1*的整数都可以唯一地分解为素数之积

证明：先证存在性，这只需用素数的定义和归纳公理即可完成。对整数$n>1$，问n是否素数？若是，则完成；若非，则存在整数a,b，使得$n=ab$。继续问：是否a和b是否都是素数，继续下去得证。

再证唯一性。设有两种分解

$$n=p_1\cdots p_s=q_1\cdots q_t,$$

则$p_1|q_1\cdots q_t$，用推论知由此推出p_1整除某一q_i，不妨设$p_1|q_1$，再由p_1,q_1是素数知$p_1=q_1$。因此

$$p_2\cdots p_s=q_2\cdots q_t,$$

归纳即可完成证明。

可见引理1.1.2是证明的关键。由唯一分解定理可知若正整数$p_1^{r_1}\cdots p_n^{r_n}$ （$r_i\ge 0$, p_i为素数）的因子一定形如$p_1^{s_1}\cdots p_n^{s_n}$ （$s_i\le r_i$）。对$a=p_1^{\alpha_1}\cdots p_n^{\alpha_n}, b=p_1^{\beta_1}\cdots p_n^{\beta_n}$，一定有

$$(a,b)=p_1^{\min(\alpha_1,\beta_1)}\cdots p_n^{\min(\alpha_n,\beta_n)}$$

$$[a,b]=p_1^{\max(\alpha_1,\beta_1)}\cdots p_n^{\max(\alpha_n,\beta_n)}$$

4 应用举例

例1、正的有理数有唯一的既约分数表示。

证明：设$\alpha=\frac{a}{b}=\frac{c}{d},(a,b)=(c,d)=1$，则$ad=bc$，那么$a|bc$，结合$(a,b)=1$知$a|c$同理$c|a$,故$a=c$,进而$b=d$，即有理数$\alpha$有唯一的既约分数表示。

例2、若$(a,b)=1$，则$(a+b,a-b)=1$或2。

证明：设$(a+b,a-b)=d$，则$d|a+b+(a-b)=2a,d|a+b-(a-b)=2b$，因此$d|(2a,2b)=2$。

例3、对任意正整数n，1000^n-1不整除1978^n-1

证明：假设$1000^n-1|1978^n-1$，则$1000^n-1|1978^n-1-(1000^n-1)=1978^n-1000^n=2^n(989^n-500^n)$，但$(1000^n-1,2^n)=1$，故$1000^n-1|989^n-500^n$。而这是不可能的，因为$0<989^n-500^n<1000^n-1$。

例4、证明对任意正整数n，不成立$7^n|9^n-1$

证明：若$7^n|9^n-1$，则$7|(3^n+1)(3^n-1)$，但$(3^n+1,3^n-1)=(3^n-1,2)=2$，故7只能整除$3^n+1$与$3^n-1$中的一个，即

$$7|3^n+1,(7,3^n-1)=1$$

或

$$7|3^n-1,(7,3^n+1)=1$$

若前者成立，则$7^n|3^n+1$ (比较大小知道不可能);若后者成立，则$7^n|3^n-1$ (同样不可能)

例5、对素数p和整数$1<r<p$，p整除组合数$\binom{p}{r}$

证明：因为$\binom{p}{r}$是整数，故$r!|p(p-1)\cdots(p-r+1)$，但因$r!$是一些小于p的数（因此非p的倍数的数）相乘，所以$r!$非p的倍数，那么$(r!,p)=1$。结合前面两式知$r!|(p-1)\cdots(p-r+1)$，所以$p|\binom{p}{r}$

例6、设a,b,c为正整数，$(a,b)=1$，$ab=c^n$，则$a=c_1^n,b=c_2^n$。

证明：设

$$a=p_1^{\alpha_1}\cdots p_r^{\alpha_r}$$

$$b=q_1^{\beta_1}\cdots q_s^{\beta_s}$$

$$c=p_1^{l_1}\cdots p_r^{l_r}q_1^{m_1}\cdots q_s^{m_s}$$

带入$ab=c^n$并比较得n整除所有α_i和β_j，即a,b都是n次幂。

例7、求方程$x^2+y^2=z^2$的整数解

解：先简化为这种特殊情形：$x>0,y>0,z>0$，x,y,z两两互素。这样x,y,z必须两奇一偶，通过考察用4除的余数知必须z奇，不失一般性可设x偶，y奇。将方程变形为

$$x^2=z^2-y^2$$

$$(\frac{x}{2})^2=(\frac{z+y}{2})(\frac{z-y}{2})$$

但由$(z,y)=1$利用例2知$(\frac{z+y}{2},\frac{z-y}{2})=1$,再由例6知

$$\frac{z+y}{2}=a^2,\frac{z-y}{2}=b^2,x=2ab$$

解为$x=2ab, y=a^2-b^2, z=a^2+b^2$，$(a,b)=1$ 要得全部解，可乘任意整数。

例8、证明奇数的平方被8除必余1

这是因为在模8的世界就只有8个数（模8有8个剩余类），其中有4个奇数1，3，5，7，依次验证可证。

例9：证明$(2^a-1, 2^b-1)=2^{(a,b)}-1$

证明：首先显然有$2^{(a,b)}-1|(2^a-1, 2^b-1)$，再证明反过来的整除关系，记$n=(2^a-1, 2^b-1)$，需证$n|2^{(a,b)}-1$，即

$$2^{(a,b)} \equiv 1 \pmod{n}$$

但

$$2^a \equiv 1 \pmod{n}$$

$$2^b \equiv 1 \pmod{n}$$

且$(a,b)=au+bv$。不难得到最后的结论。

例10、有理数的以下两种常见的定义等价

1) 可以表为分数形式.

2) 可以表为有限小数或无限循环小数的形式.

整个证明的关键是以下两种数可以互相转化:

1) 既约真分数$\frac{n}{m}$，$(m,10)=1$.

2) 纯循环小数。

纯循环小数化为分数是分析方法，1)型的既约真分数化为循环小数是找到r使得$m|10^r-1$，即

$$10^r \equiv 1 \pmod{m}$$

由于模m只有m个类，所以在序列

$10, 10^2, 10^3, ...$中必有模m重复的，即存在$i<j$有

$$10^i \equiv 10^j = 10^i \times 10^{j-i} \pmod{m}$$

故

$$10^{j-i} \pmod{1} \pmod{m}$$

这里用到了推理

$$(a,m)=1, ax \equiv ay \pmod{m} \Longrightarrow x \equiv y \pmod{m}$$

5 进一步的思考

1。唯一分解定理及证明方法在高等代数中多项式的唯一分解中出现过，这里的带余除法是利用整数的绝对值去量整数的大小；那里是用多项式的次数去量多项式的大小。

2。将视野扩展到所谓Gauss整数集合$\mathbb{Z}[i]=\{a+bi|a,b\in\mathbb{Z}\}$，在$\mathbb{Z}[i]$上容易定义整除的概念，请问

(1) $\mathbb{Z}[i]$中哪些元可以求倒数（还在$\mathbb{Z}[i]$中）

(2) 可否在$\mathbb{Z}[i]$上定义“素数”的概念。

(3) $\mathbb{Z}[i]$中的“素数”长的什么样，特别地通常的素数中哪些在$\mathbb{Z}[i]$中依然是“素数”

(4) 还有没有唯一分解定理，该如何叙述？

3。例7的解很容易转化为求圆周$x^2+y^2=1$上的有理点。请用通过点(-1,0)引直线与圆相交的方法去找出全部有理点，并想想这样的方法可否推广？

4. 证明方程$x^4+y^4=z^2$无正整数解。

6 素数分布

定理6.1. *素数有无限个。*

证明：只需证明任意大的表都不能包括全部素数。设$p_1,p_2,...,p_k$是前k个素数，则$p_1p_2\cdots p_k+1$不含这k个中任意一个作为素因子，故它的素因子必为新的素数。

定理6.2. *$4n-1$形素数有无限个。*

证明：设$p_1,p_2,...,p_k$是前k个$4n-1$形素数，考察$4p_1p_2\cdots p_k-1$，它必有一个$4n-1$形素因子，这个素因子必为新的。

定理6.3. *若$(a,b)=1$,则$a+bn$形素数有无限个。*

（这个定理的证明较深，现在没法证）

定理6.4. *存在任意长度的等差数列，全是素数。*

这个定理是获Fields奖的工作。素数分布是数论中两类最基本的问题之一:还有大量的超难的未解决问题，比如Goldbach猜想和孪生素数猜想

7 一次不定方程

数论中最重要的问题除了素数分布，还有不定方程：即解那些未知数较多（比方程个数）的方程的整数解或有理数解。最简单的当然是线性方程

$$a_1x_1+\cdots+a_rx_r=n \tag{1}$$

其中$a_1,...,a_r$不全为0 我们将从三个方面研究：判别何时有整数解，解的形状及何时有非负整数解。

定理7.1. *方程(1)有整数解当且仅当$(a_1,...,a_r)|n$*

证明：判别方程何时有解实际上是对集合$A=a_1\mathbb{Z}+\cdots+a_r\mathbb{Z}$进行分析，只要能说明有$d$使$A=d\mathbb{Z}$即可。注意$A$的简单性质：对加法运算封闭，也对整数倍（包括负的倍数）运算封闭。

取d是A中的最小正元，显然$A\supset d\mathbb{Z}$，如反包含不成立，则可取$a\in A$满足$a\notin d\mathbb{Z}$，做带余出发有$a=dq+b,0<b<d$，由A的性质知$b=a-dq\in A$，与d的最小性矛盾，说明$A=d\mathbb{Z}$。易知d必为最大公约数$(a_1,...,a_r)$。定理证必。

请在$r=2$时与定理1.1.1进行比较。现在集中关心二元方程

$$ax+by=n \tag{2}$$

不失一般性可设$(a,b)=1$，有下列定理

定理7.2. *若(x_0,y_0)为方程(1)的一组整数解，则全部解为$x=x_0+bt,y=y_0-at,t\in\mathbb{Z}$*

证明：由方程$ax+by=ax_0+by_0$得$a(x-x_0)=b(y_0-y)$,这样，$b|a(x-x_0)$，而$(a,b)=1$，故$b|x-x_0$，因此可设$x-x_0=bt$，即$x=x_0+bt$，$y=y_0-bt$

下面讨论对a,b,n都为正时，方程何时有非负整数解。显然，当n充分大时是有的，于是可以问对确定的互素的正整数a,b，最大的使方程(2)无非负整数解的n是多少？

定理7.3. *当$n = ab - a - b$时，方程(2)无非负整数解，而当$n > ab - a - b$时，方程(2)一定有非负整数解。*

证明之前先看具体例子，若$a = 8, b = 15$，那么$ab - a - b = 97$，将n分别取97和100。

先解方程$8x + 15y = 97$。取适当的x，使$97 - 8x$是15的倍数，即$8x \equiv 97 \equiv 7 \pmod{15}$，$8x \equiv -8 \pmod{15}$。由于$(8, 15) = 1$，故得$x \equiv -1 \equiv 14 \pmod{15}$. 即非负的$x$至少是14，$x$和$y$当然是一个变大，一个变小，因此要保持$x$非负，$y$至多是$\frac{97-8\times 14}{15} = -1$。因此没有让$x, y$都非负的解。

再解$8x + 15y = 100$，还是模15知$8x \equiv 100 \pmod{15}$, $2x \equiv 25 \equiv 10 \pmod{15}$, $x \equiv 5 \pmod{15}$，故可取$x = 5$，代入得$y = 4$。于是得到了x, y都非负的解。

通过例子已经有了定理证明的思想。定理证明：先考察方程

$$ax + by = ab - a - b \tag{3}$$

对x的要求是$ax \equiv ab - a - b \equiv a \pmod{b}$,即$x \equiv -1 \pmod{b}$，因此最小的非负的$x$是$b - 1$，此时$y = -1$。说明方程(3)无$x, y$均非负的解。

现考察方程(2)在$n > ab - a - b$时的解，取r为使y为整数的最小x，那么$0 \le r \le b - 1$，此时$y = \frac{n-ar}{b} > \frac{ab-a-b-a(b-1)}{b} = -1$，但因$y$为整数，故$y \ge 0$。证毕。

问题：上一个定理能否推广到三个以上未知数的情形？

练习

1、证明若$(a, m) = 1$，则

$$ax \equiv ay \pmod{m} \Longleftrightarrow x \equiv y \pmod{m}$$

如果去掉条件$(a, m) = 1$，结论是否成立？

2、求下列同余方程的解：

1) $8x \equiv 1 \pmod{13}$

2) $81x \equiv 1 \pmod{161}$

3、利用Euclid算法求391与483的最大公约数并将之表为$391u + 483v$的形式。

4、求方程$41x - 114y = 5$的一组整数解。

5、求方程$5x + 13y = 61$的全部整数解和非负整数解。

6、求满足下列条件的正整数n:

1) $n - 2 | n^2 + n + 1$

2) $2n - 1 | n^3 - n$

7、自学关于素数判别的Eratosthenes筛法并应用此法找：1000以下的最大的平方数n满足$n \pm 2$皆为素数。

8、设n是正整数，证明$\frac{21n+4}{14n+3}$是既约分数。

9、设n是正整数，证明若$\sqrt{n}$是有理数，则是整数。

10、证明若a为奇数，b为整数，则$(a, b) = (a, 2b)$。

11、设m, n为正整数，m为奇，证明$2^m - 1$与$2^n + 1$互素。

同余式

第二周 同余的几个基本定理

8 Euler定理和Fermat小定理

基本概念：将集合$a+m\mathbb{Z}$（可简记为$\overline{a}$）称为一个模m的剩余类，a称为这个剩余类的一个代表元。显然一个剩余类中任何元与m的最大公约数都相同，因此我们可以说：某个剩余类与m互素。模m的剩余类有m个，可记为$\overline{0},\overline{1},...,\overline{m-1}$，其中与$m$互素的类的个数记为$\phi(m)$，这个函数$\phi$称为Euler函数。对素数$p$，$\phi(p)=p-1$，$\phi(p^n)=p^{n-1}$。另外若有$a_1,...,a_m$分别是模$m$的各个剩余类的一个代表元，称$a_1,...,a_m$组成一个模$m$的完全剩余系；另外若有$a_1,...,a_{\phi(m)}$分别是模$m$的各个与$m$互素的剩余类的一个代表元，称$a_1,...,a_{\phi(m)}$组成一个模$m$的（完全）剩余缩系；对与$m$互素的$a$，将最小的满足$a^r\equiv 1 \pmod m$的正整数$r$称为$a$模$m$的阶。

请牢记并熟练运用一个常用的结论：

若$(a,m)=1$，则同余方程$ax\equiv b \pmod m$有唯一解。这是因为在模m的世界与m互素的数都可以求“倒数”，这将被频繁用到，也是前面证明唯一分解定理的关键。

定理8.1. *Euler定理。对整数a,m，若$(a,m)=1$，则有$a^{\phi(m)}\equiv 1 \pmod m$*

证明：取$a_1,a_2,...,a_{\phi(m)}$为模m的一组剩余缩系，则$aa_1,aa_2,...,aa_{\phi(m)}$为另一组剩余缩系，因此

$$a_1a_2\cdots a_{\phi(m)}\equiv aa_1aa_2\cdots aa_{\phi(m)}\equiv a^{\phi(m)}a_1a_2\cdots a_{\phi(m)}$$

所以$a^{\phi(m)}\equiv 1 \pmod m$。

将m取为素数p，就得到Fermat小定理（得名是因为区别于Fermat大定理）

定理8.2. *Fermat小定理。对素数p，若$(a,p)=1$，则有$a^{p-1}\equiv 1 \pmod p$*

这个定理也可叙述为如下版本

对任意素数p和整数a，有

$$a^p\equiv a \pmod p$$

应用举例：

1. 对任意整数a，有

$$a^9\equiv a^3 \pmod{7\times 8\times 9}$$

证：这需要分别证明三个同余式

$$a^9\equiv a^3 \pmod 7$$

$$a^9\equiv a^3 \pmod 8$$

$$a^9\equiv a^3 \pmod 9$$

由Fermat小定理直接有

$$a^7\equiv a \pmod 7$$

故得第一个。第二个分a奇和a偶两种情形。在奇情形，由$a^2\equiv 1 \pmod 8$立得；偶情形则直接验证。第三个按a是否3的倍数分两种情形，一种直接验证，一种由Euler定理得到。

2. 研究$\frac{1}{7},\frac{1}{17},\frac{1}{7^2}$各是多少位循环小数。

分析：首先既约分数$\frac{n}{m}$的循环小数的长度就是最小的满足$m|10^r-1$的正整数r，即10模m的阶，经过简单计算可知10模7的阶是6，因此$\frac{1}{7}$是6位循环小数。$\frac{1}{17}$的计算量大一些，由Fermat小定理知长度$r|16$，因此只需计算如下部分：

$$10^2\equiv -2 \pmod{17}$$

$$10^4 \equiv (-2)^2 \equiv 4 \pmod{17}$$

$$10^8 \equiv 16 \equiv -1 \pmod{17}$$

故$r = 16$，即$\frac{1}{17}$是16位循环小数；再研究$\frac{1}{7^2}$，设它的循环小数长度是r，通过Euler定理（详细说明自己补充）可知

$$6|r|7 \times 6$$

从而有$r = 6$或42，但$r \neq 6$（经简单计算知$10^6 \not\equiv 1 \pmod{49}$）。故$\frac{1}{7^2}$是42位循环小数。在我们的推理中用到了下列简单命题（略去证明）

命题8.3. *对整数a, m，若$(a, m) = 1$，a模m的阶是r，则对整数n有*

$$a^n \equiv 1 \pmod{m} \Longleftrightarrow r|n$$

定理8.4. *Wilson定理。对任意素数p，有$(p-1)! \equiv -1 \pmod{p}$*

证明：当$p = 2$时，显然成立，现在设p为奇素数。对任意$i \in A = \{1, 2, ..., p-1\}$，存在唯一$i' \in A$满足$ii' \equiv 1 \pmod{p}$。将每个$i$与$i'$配成一对，但当$i = i'$，即$i^2 \equiv 1$时，无其他元与$i$配对。故

$$(p-1)! = \prod_{i \in A} i \equiv \prod_{i \in A, i^2 \equiv 1 \pmod{p}} i \equiv 1 \times (-1) \equiv -1 \pmod{p}$$

应用：对素数$p \equiv 1 \pmod{4}$，存在整数a使得$p|a^2 + 1$

证明：由于$(p-i) \equiv -i \pmod{p}, i = 1, ..., \frac{p-1}{2}$，故$(p-1)! \equiv (\frac{p-1}{2})!(-1)^{\frac{p-1}{2}}(\frac{p-1}{2})! \equiv ((\frac{p-1}{2})!)^2 \pmod{p}$，结合Wilson定理知$((\frac{p-1}{2})!)^2 \equiv -1 \pmod{p}$，即$p|((\frac{p-1}{2})!)^2 + 1$

思考题：如何将Wilson定理推广到模奇素数幂的情形。

9 孙子定理

现实或理论中都常遇到解不同模的同余式组

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ \cdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

这个问题的简单回答是：只要$m_1, m_2, ..., m_n$两两互素，则（不论$a_1, ..., a_n$如何取）同余式组一定有解，且解是一个模$m = m_1 \cdots m_n$的剩余类。假如找到一个解a，显然剩余类$a + m\mathbb{Z}$中的元都是解，另外由$x \equiv a_i \equiv a \pmod{m_i}$得到$m_i|x - a$，由$m_i$两两互素知$m|x - a$，即$x \equiv a \pmod{m}$。中国古人的贡献是找到一种有效的解法，即所谓的孙子定理，外国称为中国剩余定理（Chinese remainder theorem）。

定理9.1. *设$m_1, m_2, ..., m_n$两两互素，$m = m_1 \cdots m_n$，$M_i = \frac{m}{m_i}$，则上述同余式组的解是*

$$x \equiv a,$$

$$a = a_1 M_1' + \cdots + a_n M_n',$$

$$M_i M_i' \equiv 1 \pmod{m_i}$$

证明：首先将原始的同余式组归结到n个特殊情形，即

$$\begin{cases} x \equiv 0 \pmod{m_1} \\ \cdots \\ x \equiv a_i \pmod{m_i} \\ \cdots \\ x \equiv 0 \pmod{m_n} \end{cases}$$

$i = 1, ..., n$，只要将n个解相加即可。然后继续简化为：

$$\begin{cases} x \equiv 0 \pmod{m_1} \\ \cdots \\ x \equiv 1 \pmod{m_i} \\ \cdots \\ x \equiv 0 \pmod{m_n} \end{cases}$$

只要将每个解乘上a_i。而最后一个组简化为：

$$\begin{cases} x \equiv 1 \pmod{m_i} \\ x \equiv 0 \pmod{M_i} \end{cases}$$

而这又化为解$M_i y \equiv 1 \pmod{m_i}$。有解性由$(m_i, M_i) = 1$保证。当得到最后一个的解$M_i'$，倒回去即得定理的证明。

注：证明的第一部分，即说明同余式组的解（若有）一定是模$m_1 \cdots m_n$的一个剩余类相当于线性方程求解时，将问题归结为齐次方程的通解和原方程的特解；第二部分相当于向量恒等式

$$(a_1, ..., a_n) = a_1(1, 0, ..., 0) + \cdots + a_n(0, ..., 0, 1)$$

例：解方程

$$\begin{cases} x \equiv 2 \pmod{4} \\ x \equiv 3 \pmod{25} \end{cases}$$

解：先解$4x \equiv 1 \pmod{25}$ 得$x \equiv 19 \pmod{25}$；再解$25x \equiv 1 \pmod{4}$得$x \equiv 1 \pmod{4}$。于是得到

$$\begin{cases} 76 \equiv 0 \pmod{4} \\ 76 \equiv 1 \pmod{25} \end{cases}$$

$$\begin{cases} 25 \equiv 1 \pmod{4} \\ 25 \equiv 0 \pmod{25} \end{cases}$$

原同余式组的解是

$$x \equiv 2 \times 25 + 3 \times 76 \equiv 78 \pmod{100}$$

例: 求$76^{2009} + 25^{2009}$的最后两位数字。

解：由

$$\begin{cases} 76 \equiv 0 \pmod 4 \\ 76 \equiv 1 \pmod{25} \end{cases}$$

知$76^2 \equiv 76 \pmod{100}$，同理$25^2 \equiv 25 \pmod{100}$。故

$$76^{2009} + 25^{2009} \equiv 76 + 25 \equiv 1 \pmod{100},$$

因此，最后两位数字是0和1。实际上76和25就是通过$x^2 - x \equiv 0 \pmod{100}$解出的。

例求满足$mn - 1 | n^3 + 1$的正整数对(m, n)。

解：易知$mn - 1 | n^3 + 1$等价于$mn - 1 | m^3 + 1$，故m和n的地位相等，可设$m \geq n$。若$m = n$，可得$m = n = 2$；若$m > n$，则$\frac{n^3+1}{mn-1} < n$，另外$\frac{n^3+1}{mn-1} \equiv -1 \pmod n$，故$\frac{n^3+1}{mn-1} = n - 1$，由$n - 1 | n^3 + 1$可知$n - 1 | 2$，即$n = 2, 3$，相应地$m = 5$。综上，所有可能的$(m, n)$为$(1, 1), (5, 2), (5, 3), (2, 5), (3, 5)$。

10 Euler函数的计算

Euler函数的计算。我们用两种方法计算出

$$\phi(n) = n \prod_{p|n} (1 - \frac{1}{p})$$

方法一：设n的素因子全体为$p_1, ..., p_r$，从1到n中p_i的倍数组成的集合是C_i，那么

$$\phi(n) = n - |C_1 \bigcup \cdots \bigcup C_r|$$

再由容斥原则知：

$$\phi(n) = n - \sum_{1 \leq i \leq r} \frac{n}{p_i} + \cdots + (-1)^r \frac{n}{p_1 \cdots p_r} = n \prod_{1 \leq i \leq r} (1 - \frac{1}{p_i})$$

即

$$\phi(n) = n \prod_{p|n} (1 - \frac{1}{p})$$

方法二：现有$\phi(p^l) = p^l - p^{l-1}$（显然），再证明Euler函数具有乘性，即对整数$m_1, m_2$互素，有：

$$\phi(m_1 m_2) = \phi(m_1)\phi(m_2)$$

取集合A, A_1, A_2分别为模$m = m_1 m_2$，模m_1，模m_2的各一组完全剩余系，做A到$A_1 \times A_2$的映射$\sigma : a \longmapsto (a_1, a_2)$,其中$a_i$由$a \equiv a_i \pmod{m_i}$确定。这个映射显然是单的，因为

$$a \equiv b \pmod{m_i}, i = 1, 2 \Longrightarrow a \equiv b \pmod m$$

另外，因A与$A_1 \times A_2$均是有限集，且元素个数相等，故σ是双射（本质上这就是孙子定理）。取集合$B \subset A$，$B_1 \subset A_1$，$B_2 \subset A_2$分别是模m，模m_1，模m_2的一组剩余缩系，则由

$$(a, m) = 1 \Longleftrightarrow (a, m_1) = (a, m_2) = 1 \Longleftrightarrow (a_1, m_1) = (a_2, m_2) = 1$$

知σ在B上的限制给出B到$B_1 \times B_2$的一一对应。因此元素个数相等，故$\phi(m_1 m_2) = \phi(m_1)\phi(m_2)$

Euler函数有一重要性质：

$$\sum_{d|n} \phi(d) = n$$

证明：将n以内的正整数x按(x,n)分类。记$A=[1,n]\cap\mathbb{Z}$，$A_d=\{x\in A|(x,n)=d\}$. 由于

$$(x,n)=d\Longleftrightarrow x=dy,d|n,(y,\frac{n}{d})=1$$

故$|A_d|=\phi(\frac{n}{d})$。因为$A=\cup_{d|n}A_d$，两边数数可得

$$n=\sum_{d|n}\phi(\frac{n}{d})=\sum_{d|n}\phi(d)$$

练习

1、找出$(1,1000)$内的整数，满足：任意方幂的末尾三位数字都不变。类推，证明：对任意n，存在正好两个整数a,b在2与10^n之间，任意方幂的末尾n位数字都不变，进一步请问$a+b$是多少？
2、证明:若$(a,b)=1$，则$(a-b,\frac{a^p-b^p}{a-b})=1$或$p$。
3、$\frac{1}{49},\frac{1}{91}$各是多少位循环小数？
4、求满足$7|2^n-n^2$的全部n
5、求满足$ab^2+b+7|a^2b+a+b$的所有正整数a,b。
6、设p是素数，若$a\equiv b\not\equiv 0\pmod p$，证明对任意$n$，有

$$\mathrm{ord}_p(a^n-b^n)=\mathrm{ord}_p(a-b)+\mathrm{ord}_p n$$

一般地，$\mathrm{ord}_p m$定义为最大的满足$p^r|m$的r。
以下是书中第一章3、4、7、11、14、15、22、29、33，第二章3、4、5、14、17、20、22(1)、24(1)(2)。

思考题：
1、设a,b为正整数，证明若$\frac{a^2+b^2}{ab+1}$为整数，则为平方数。
2、对什么正整数a,b，有$ab|a^2+b^2+3$。

第三周 同余方程

11 同余方程的解法

设有整系数多项式$f(X)$（我们约定用大写字母表多项式的未定元），经常会遇到下列的同余方程

$$f(x)\equiv 0\pmod m \tag{1}$$

约定：当我们说方程(1)有n个解时，指的是在$[0,m-1]$中有n个解，或等价地指所有解有n个模m的剩余类。例如：方程$2x-4\equiv 0\pmod 8$等价于方程$x-2\equiv 0\pmod 4$，但按约定应该说前者有两个解，后者有一个解。另外，对整系数多项式$f(X)$，$g(X)$，记号

$$f(X)\equiv g(X)\pmod m$$

表示f和g的定义系数同余，换句话说，存在整系数多项式$h(X)$，使得

$$f(X)=g(X)+mh(X)$$

一个基本问题是如何解方程(1)，一个万能的解法是穷举，但即使这样，也应当设法使穷举范围缩小，于是有以下方案：

第一步：将m分解为$m = p_1^{l_1} \cdots p_r^{l_r}$，从而将(1)化为$r$个方程

$$f(x) \equiv 0 \pmod{p_i^{l_i}}, i = 1, ..., r$$

如果得出上述方程的各一个解$x \equiv a_i \pmod{p_i^{l_i}}$，再用孙子定理可解出(1)的一个模$m$的解。

定理11.1. *如果方程*

$$f(x) \equiv 0 \pmod{p_i^{l_i}}$$

有n_i个解，$i = 1, ..., r$，$m = p_1^{l_1} \cdots p_r^{l_r}$，则方程(1)有$n_1 \cdots n_r$个解

证明:由孙子定理立得。

例1、解方程$x^2 - x \equiv 0 \pmod{100}$

解：先解$x^2 - x \equiv 0 \pmod 4$和$x^2 - x \equiv 0 \pmod{25}$，分别得到$x \equiv 0, 1 \pmod 4$和$x \equiv 0, 1 \pmod{25}$。再通过孙子定理得到四个解$x \equiv 0, 1, 76, 25 \pmod{100}$

总之我们将一般的方程(1)简化为解模素数幂的方程。

第二步：将模素数幂的方程简化为模素数的方程

由于

$$f(x) \equiv 0 \pmod{p^l} \Longrightarrow f(x) \equiv 0 \pmod{p^{l-1}}$$

因此我们在解方程$f(x) \equiv 0 \pmod{p^l}$时，应该逐次解

$$f(x) \equiv 0 \pmod p, f(x) \equiv 0 \pmod{p^2}, ...$$

著名的Hensel引理是说从$f(x) \equiv 0 \pmod p$的一个好的解可以提升得到$f(x) \equiv 0 \pmod{p^l}$的一个解。

引理11.2. *Hensel引理。如果整数a_0满足$f(a_0) \equiv 0 \pmod p$，而$f'(a_0) \not\equiv 0 \pmod p$，则存在唯一的整数序列$a_1, a_2, ...$, $0 \le a_i \le p - 1$使对任意$l > 1$,方程(2)*

$$\begin{cases} f(x) \equiv 0 \pmod{p^l} \\ x \equiv a_0 \pmod p \end{cases}$$

有唯一解$x \equiv a_0 + a_1 p + \cdots + a_{l-1} p^{l-1} \pmod{p^l}$

这个引理的证明就是逐次解方程$f(x) \equiv 0 \pmod{p^l}, l = 2, 3, ...$。记$x = a_0 + px_1$，代入方程$f(x) \equiv 0 \pmod{p^2}$得$f(a_0 + px_1) \equiv f(a_0) + f'(a_0)px_1 \equiv 0 \pmod{p^2}$, 因此$f'(a_0)x_1 \equiv -\frac{f(a_0)}{p} \pmod p$。有唯一解，记为$x_1 \equiv a_1 \pmod{p^2}$。得到方程(2)在$l = 2$时的唯一解$x \equiv a_0 + a_1 p$。第归地解方程，若解出$x \equiv \alpha_{l-2} = a_0 + a_1 p + \cdots + a_{l-2} p^{l-2} \pmod{p^{l-1}}$为

$$\begin{cases} f(x) \equiv 0 \pmod{p^{l-1}} \\ x \equiv a_0 \pmod p \end{cases}$$

的解，设$x = \alpha_{l-2} + p^l x_{x_l}$，代入(2)并化简得$f'(\alpha_{l-2})x_{l-1} \equiv -\frac{f(\alpha_{l-2})}{p} \pmod p$，也有唯一解（因$f'(\alpha_{l-2}) \equiv f'(a_0) \not\equiv 0 \pmod p$）$x_{l-1} \equiv a_{l-1} \pmod p$，由此得到(2)的唯一解

$$x \equiv \alpha_{l-2} + p^{l-1} a_{l-1} = a_0 + a_1 p + \cdots + a_{l-1} p^{l-1} \pmod{p^l} \pmod{p^l}$$

例2、解同余方程

$$7x^4+19x+25\equiv 0 \pmod{27}$$

解：先解

$$7x^4+19x+25\equiv 0 \pmod{3}$$

易知有唯一解$x\equiv 1 \pmod 3$。令$x=1+3y$，代入

$$7x^4+19x+25\equiv 0 \pmod{9} \tag{3}$$

并化简得$6+6y\equiv 0 \pmod 9$，即$y\equiv 2 \pmod 3$。那么(3)的解为$x\equiv 7 \pmod 9$。再设$x=7+9z$，代入原方程并化简得$18+9z\equiv 0 \pmod{27}$，解得$x\equiv 1 \pmod 3$。因此原方程有唯一解

$$x\equiv 16 \pmod{27}$$

例3、方程$x^{p-1}-1\equiv 0 \pmod{p^l}$

解：由Fermat小定理知$f(x)=x^{p-1}-1\equiv 0 \pmod p$有$p-1$个解$1,2,...,p-1$，但$f'(x)\equiv -x^{p-1}$，故每个解都满足Hensel引理的条件，故都可得到原方程的唯一一个解，于是原方程有$p-1$个解。

模素数的同余方程并没有一个万能解法（除了穷举），但有如下定性结论

定理11.3. 拉格朗日定理。如果方程$f(x)\equiv 0 \pmod p$解数不超过$f(x)$的次数$degf$

这个定理的证明与通常证明一个数域上的代数方程相应结论是一样的。因为

$$ab\equiv 0 \pmod p \Longrightarrow a\equiv 0 \pmod p \text{或} \equiv 0 \pmod p$$

因此对任意整系数多项式$f(X),g(X)$，有

$$\{x\in\mathbb{Z}|f(x)g(x)\equiv 0 \pmod p\}=\{x\in\mathbb{Z}|f(x)\equiv 0 \pmod p\}\cup\{x\in\mathbb{Z}|g(x)\equiv 0 \pmod p\},$$

另一方面，由于任何$f(X)$总可表为$f(X)=(X-a)g(X)+f(a)$，故可得

$$f(a)\equiv 0 \pmod p \Longleftrightarrow \text{存在}g(X),\text{满足}f(X)\equiv (X-a)g(X) \pmod p$$

用以上两点通过归纳法可得定理证明。

这个定理有很多有趣的重要应用。首先可以重证Wilson定理：由Fermat小定理知$x^{p-1}-1\equiv 0 \pmod p$有$p-1$个根$1,2,...,p-1$，再用拉格朗日定理知必有

$$X^{p-1}-1\equiv (X-1)(X-2)\cdots(X-(p-1)) \pmod p$$

比较常数项知

$$-1\equiv (-1)^{p-1}(p-1)!\equiv (p-1)! \pmod p$$

还可以证明下列结论：

定理11.4. 对正整数$d|p-1$，有

*(1)*方程$x^d-1\equiv 0 \pmod p$恰有d个根

*(2)*对给定整数a，若存在b满足$a\equiv b^d$，则称a是模p的d次剩余。

$$a\text{是}d\text{次剩余}\Longleftrightarrow a^{\frac{p-1}{d}}\equiv 1 \pmod p$$

证明：(1)因为$x^{p-1}-1\equiv 0 \pmod p$有$p-1$个根，而$x^d-1$是$x^{p-1}-1$的因子，由拉格朗日定理立得$x^d-1\equiv 0 \pmod p$的根数亦为次数，即$d$。
(2)先证$\Longrightarrow$. 若$a\equiv b^d$，则$a^{\frac{p-1}{d}}\equiv b^{p-1}\equiv 1 \pmod p$。然后证明满足两边条件的数（在一个剩余系内）一样多。由(1)已知右边的有$\frac{p-1}{d}$个。为数左边，写出全部d次剩余$1^d,2^d,...,(p-1)^d$，这$p-1$个列出的对象并不表示$p-1$个剩余类。因为对任意b，满足$x^d\equiv b^d \pmod p$的x恰有d个类$x\equiv b\alpha_i, i=1,...,d$，这里$\alpha_i$表$x^d-1\equiv 0 \pmod p$的那$d$个根。说明$1^d,2^d,...,(p-1)^d$中每$d$个同余，那么$d$次剩余一共是$\frac{p-1}{d}$个。

12 典型例子

例1、什么正整数n，可唯一表为$\frac{x^2+y}{xy+1}$，x,y为正整数。
解：先做实验。$n=1$时显然不唯一，因为由$\frac{x^2+y}{xy+1}=1$得$y=x+1$，解数无限。$n=2,3$时可验证唯一可表，现证$n>1$均可：将方程$\frac{x^2+y}{xy+1}=n$变形为

$$y=\frac{x^2-n}{nx-1} \tag{1}$$

要$y\geq 1$，必须$x>n$。同时，由(1)知

$$\frac{n^3-1}{nx-1}$$

也应为整数，因

$$x^2\equiv n \pmod{nx-1} \Longrightarrow n^3\equiv n^2x^2\equiv 1 \pmod{nx-1}$$

我们来说明$d:=\frac{n^3-1}{nx-1}=1$，首先$d<n$（因$x>n$），其次$d\equiv 1 \pmod n$。方程的解为

$$x=n^2, y=n$$

对任意整数a和素数p，可定义$\mathrm{ord}_p a$，且有如下性质：
(1) $\mathrm{ord}_p ab=\mathrm{ord}_p a+\mathrm{ord}_p b$,
(2) $\mathrm{ord}_p(a+b)\geq \min(\mathrm{ord}_p a,\mathrm{ord}_p b)$, 且在$\mathrm{ord}_p a\neq \mathrm{ord}_p b$时，一定取等号。这些事实容易验证，还可推广到$a$为有理数时，只要规定

$$\mathrm{ord}_p\frac{n}{m}=\mathrm{ord}_p n-\mathrm{ord}_p m$$

由定义可知：
1) 对任意整数a，$\mathrm{ord}_p a\geq 0$
2) 对有理数a，$\mathrm{ord}_p a\geq 0\Longleftrightarrow a$的分母不是$p$的倍数

有了这些准备，讲几个例子：
例3、求$a=1+\frac{1}{2}+\cdots+\frac{1}{10}$的分母
解：首先，分母的素因子只能是10以内的素数，因此只要对所有10以内素数p，求出$\mathrm{ord}_p a$即可：
1) 对素数2，8是含2最多的，故

$$\mathrm{ord}_2 a=\mathrm{ord}_2\frac{1}{8}=-3$$

2) 对素数3，9是含3最多的，故

$$\mathrm{ord}_3 a=\mathrm{ord}_2\frac{1}{9}=-2$$

3) 对素数5，5和10并列含5最多，故应具体计算得

$$\mathrm{ord}_5(\frac{1}{5}+\frac{1}{10})=\mathrm{ord}_5\frac{3}{10}=-1$$

由于其余部分分母都不含5，故

$$\mathrm{ord}_5 a = -1$$

4) 只有7含有7，故

$$\mathrm{ord}_7 a = -1$$

综上，a的分母是$8 \times 9 \times 5 \times 7$.

例4、证明对$n > 1$，$a = 1 + \frac{1}{2} + \cdots + \frac{1}{n}$不是整数。

证明：对素数2讨论，象上题那样说明1到n中只有一个数含有最多的2：存在唯一的r满足$2^r \leq n < 2^{r+1}$，于是任一1到n中非2^r的其它数m，由于$1 \neq \frac{m}{2^r} < 2$，故$\frac{m}{2^r}$不是整数，因此必有$\mathrm{ord}_2 m < r$。这样，

$$\mathrm{ord}_2 a = \mathrm{ord}_2 \frac{1}{2^r} = -r$$

例5、设p是奇素数，若$a \equiv b \pmod{p}$，证明对任意n，有

$$\mathrm{ord}_p(a^n - b^n) = \mathrm{ord}_p(a-b) + \mathrm{ord}_p n$$

证明：首先注意到

$$\mathrm{ord}_p(a^{mn} - b^{mn}) - \mathrm{ord}_p(a-b) = (\mathrm{ord}_p(a^{mn} - b^{mn}) - \mathrm{ord}_p(a^n - b^n)) + (\mathrm{ord}_p(a^n - b^n) - \mathrm{ord}_p(a-b))$$

因此上述结论对m和n分别成立，则对mn成立，这样就归结为n取素数时，将n分两种情形讨论：

1) $n = q \neq p$时，

$\frac{a^q - b^q}{a-b} \equiv q a^{q-1} \not\equiv 0 \pmod{p}$，结论成立；

2) $n = p$时，需证$\mathrm{ord}_p \frac{a^p - b^p}{a-b} = 1$.

若$\mathrm{ord}_p(a-b) > 1$，即$a \equiv b \pmod{p^2}$，则

$\frac{a^p - b^p}{a-b} \equiv p a^{p-1} \not\equiv 0 \pmod{p^2}$，结论成立；

若$\mathrm{ord}_p(a-b) = 1$，可设$a \equiv b + pt \pmod{p^2}$，$t \not\equiv 0 \pmod{p}$，于是

$$a^p \equiv (b+pt)^p \equiv b^p + p^2 b^{p-1} t \pmod{p^3}$$

由于$bt \not\equiv 0 \pmod{p}$，因此上式意味着

$$\mathrm{ord}_p(a^p - b^p) = 2 = \mathrm{ord}_p(a-b) + \mathrm{ord}_p p$$

结论成立。

例5、分解整数11111。

解：只要检验$\sqrt{11111}$以内的那些素数p是否11111的因子即可，但逐一检查工作量过大，注意事实

$$11111 \times 9 = 10^5 - 1$$

可知

$$p|11111 \Longleftrightarrow p|10^5 - 1, \text{且} p \neq 3 \Longleftrightarrow 10\text{模}p\text{的阶是}5$$

因此再用Fermat小定理知对$p|11111$必然$5|p-1$，进而$p \equiv 1 \pmod{1}0$，这就大大缩小了范围，易知

$$11111 = 41 \times 271$$

练习

1. 证明若$f'(a) \equiv 0 \pmod{p}$，则

$$\begin{cases} f(x) \equiv 0 \pmod{p^2} \\ x \equiv a \pmod{p} \end{cases}$$

的解数是0或p。请各举一例。

2. 若$a_1, ..., a_n$是模p两两不同余的整数，问$(x-a_1)\cdots(x-a_n) \equiv 0 \pmod{p^3}$有多少解。

3. 方程

$$x(x-1)(x-2)(x-5) \equiv 0 \pmod{5^3}$$

有多少解。

4. 证明方程$x^{p-1} - 1 \equiv 0 \pmod{p^l}$的全部解是

$$x \equiv a^{p^{l-1}} \pmod{p^l}, a = 1, 2, ..., p-1$$

5、求$1 + \frac{1}{2} + \cdots + \frac{1}{20}$的分母。

6、书上第二章习题4、5、8、10、12、14、15、20、25

代数结构

第四周 群与数论

13 集合论预备知识

大家都知道集合、映射、关系等概念。现介绍一些常用工具：

• **交换图**。下图是关于一些集合与映射的图：

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle\phi}\downarrow & & \downarrow{\scriptstyle\psi} \\ C & \xrightarrow{g} & D \end{array}$$

我们称这个图表交换，如果$\psi \circ f = g \circ \phi$，即$A$中的元沿着两条路到达$D$得到同一个元。

• **运算**：集合S的一个运算是指一个映射$f : S \times S \longrightarrow S$。

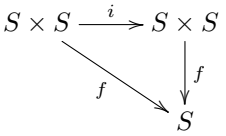
我们常常说一个运算“$\circ$”是指将(a, b)的像$f(a, b)$记作$a \circ b$。记号$\circ$不是本质，f才是。我们说运算“$\circ$”或“f”具有结合律是指对任意$a, b, c \in S$，有$(a \circ b) \circ c = a \circ (b \circ c)$，或下图交换：

$$\begin{array}{ccc} S \times S \times S & \xrightarrow{f \times 1} & S \times S \\ {\scriptstyle 1\times f}\downarrow & & \downarrow{\scriptstyle f} \\ S \times S & \xrightarrow{f} & S \end{array}$$

$(f \times 1)(a, b, c) = (f(a, b), c)$

$(1 \times f)(a, b, c) = (a, f(b, c))$.

我们说运算“$\circ$”或“f”具有交换律是指对任意$a, b \in S$，有$a \circ b = b \circ a$或下图交换：



$i(a,b)=(b,a)$

• **运算封闭**：集S上有运算“$\circ$”，我们常说S的某子集A对“$\circ$”封闭，是指对任意$a,b\in A$，都有$a\circ b\in A$。这样A就可以继承S的运算“$\circ$”。

• **等价关系与划分**：我们知道给集合X上一个等价关系$\sim$等同于给X的一个划分，即把X分解为一些不交子集的并。每个$a\in X$在一个子集（即等价类）中，记为$\overline{a}$。记

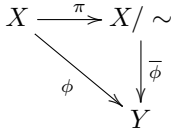
$$X/\sim:=\{\overline{x}|x\in X\},$$

称之为X对$\sim$的商集。有自然投射$\pi:X\longrightarrow X/\sim,\ x\longmapsto\overline{x}.$

命题13.1. *设有集合的映射$\phi:X\longrightarrow Y$，在X上定义等价关系$\sim$如下*

$$a\sim b\Longleftrightarrow\phi(a)=\phi(b),$$

则存在唯一映射$\overline{\phi}$使得下图交换



并且$\overline{\phi}$是单射。

命题的证明留作练习。

14 数论与群

定义14.1. *设G是一个集合，G上有一个运算$\circ$，即一个$G\times G$到G的映射，将元素对(a,b)的像记为$a\circ b$。如果运算满足以下性质三条：*
1) 结合律。对任意$a,b,c\in G$，有$(a\circ b)\circ c=a\circ(b\circ c)$
2) 单位元（或称恒等元）。存在$e\in G$，使得对任意$a\in G$，有$a\circ e=e\circ a=a$
3) 逆元。对任意$a\in G$，存在$b\in G$，使得$a\circ b=b\circ a=e$。称b为a的逆元
称G关于运算$\circ$构成一个群，或称$(G,\circ)$是一个群。有时简单地说G是一个群。如果只满足1)，称$(G,\circ)$是一个半群；如果只满足1)和2)，称$(G,\circ)$是一个幺半群。如果G已经是群，还进一步满足对任意$a,b\in G$，有$a\circ b=b\circ a$，称G是一个交换群或abel群。

注:
• 单位元是唯一的，一个元的逆元也是唯一的。
• 在群中$a\circ b=e$等价于$b\circ a=e$，这时a与b互为逆元，记$b=a^{-1}$。
• 群运算最常见的是记为乘法$\cdot$和加法$+$。但通常有个约定：只有abel群的运算才可记为加法，这时逆元记为$-a$，也会有na（n为整数，$a\in G$）的记号；如果运算记为乘法$\cdot$，常常省略$\cdot$，简单记$a\cdot b$为ab，同时有记号a^n。
• 群有如下基本性质：
对群G中任意给定的元a,b，方程$ax=b$和$ya=b$都在G中有唯一解。
• 特别地，群有消去律。

$$ax=ay\Longrightarrow x=y,xa=ya\Longrightarrow x=y$$

• 如果把群的定义中2)和3)分别改为（看视较弱的）以下
2') 左单位元e, 即对任意$a\in G$，有

$$ea=a$$

3') 左逆元，即对任意$a \in G$，存在$b \in G$，有

$$ba = e$$

依然成群，即2)，3)也满足。作为练习证明之，可参见北大代数学。

现看基本的群的例子：

例1：整数集$\mathbb{Z}$按通常的加法成为群，常称整数加群。

例2：有理数集$\mathbb{Q}$，实数集$\mathbb{R}$和复数集$\mathbb{C}$按通常的加法成为群。

例3：集合$\mathbb{Q}^*$，$\mathbb{R}^*$和$\mathbb{C}^*$按通常的乘法成为群（这里加$*$表示去掉0的剩余部分）。

以上的群都是abel群，下面看一个非交换群。

例4：k上全体n阶方阵$\mathrm{GL}_n(k)$按矩阵乘法构成的群，$k = \mathbb{Q}, \mathbb{R}$或$\mathbb{C}$。

下面两个例子是初等数论中常见的:

例5：对整数$n > 1$，$\mathbb{Z}/n\mathbb{Z}$表示集合

$$\{i + n\mathbb{Z} | i \in \mathbb{Z}\} = \{i + n\mathbb{Z} | i = 0, 1, ..., n-1\}$$

定义加法运算:$(i+n\mathbb{Z})+(j+n\mathbb{Z}) = \{x+y | x \in i+n\mathbb{Z}, y \in j+n\mathbb{Z}\} = (i+j)+n\mathbb{Z}$。现在简单记$\overline{i} = i+n\mathbb{Z}$，那么$\mathbb{Z}/n\mathbb{Z} = \{\overline{i} | i = 0, 1, ..., n-1\}$按加法成为一个abel群，以$\overline{0} = n\mathbb{Z}$为单位元。

例6：对整数$n > 1$，$\mathbb{Z}/n\mathbb{Z}$的子集合

$$\{\overline{i} | i \in \mathbb{Z}, (i, n) = 1\}$$

按照乘法运算：

$$(\overline{i})(\overline{j}) := \overline{ij}$$

构成群，也是abel群，记为$(\mathbb{Z}/n\mathbb{Z})^\times$，群的单位元是$\overline{1}$。需注意的是要验证乘法运算的合理性

$$\overline{i} = \overline{i'}, \overline{j} = \overline{j'} \Longrightarrow \overline{ij} = \overline{i'j'}$$

同时不再有

$$(\overline{i})(\overline{j}) = \{x \in \overline{i}, y \in \overline{j}\}$$

下面看一些似曾相识的群的概念和结论：

定义14.2. 设G是群（运算记为乘法，单位元为e），$a \in G$，满足$a^r = e$的最小正整数r称为a的阶。如果没有这样的r，称阶为无穷。因此将群中元素分成有限阶元和无限阶元两部分

命题14.3. 若a是群G的r阶元，则$a^n = e \Longleftrightarrow r|n$

命题14.4. 设G是n阶*abel*群（即含有n个元），则

(1)（*Euler*定理的推广）对任意$a \in G$，有$a^n = e$

(2)（*Wilson*定理的推广）G中所有元之积等于所有2阶元之积。

证明方法都完全一样。需注意(1)对非abel群也成立，只是证法不同。

命题14.5. 设G是*abel*群，$a \in G$是n阶元，则a^s的阶是$\frac{n}{(s,n)}$

证明：若$s|n$，显然a^s的阶是$\frac{n}{s}$；对一般情形，$a^{(s,n)}$的阶是$\frac{n}{(s,n)}$，我们只需说明a^s的阶与$a^{(s,n)}$的阶相同即可，这可以由这两个元互为方幂关系得到（因为“s和(s,n)在模n的世界互为倍数关系”）

命题14.6. 设G是*abel*群，若$a \in G$是m阶元，$b \in G$是n阶元，且n和m互素，则ab的阶是mn

证明：我们证对任意整数s，有

$$(ab)^s = e \Longleftrightarrow mn|s$$

首先“$\Longleftarrow$”是显然的，其次

$$(ab)^s = e \Longrightarrow (ab)^{sn} = e \Longrightarrow a^{sn} = e \Longrightarrow m|sn \Longrightarrow m|s$$

同理

$$(ab)^s = e \Longrightarrow n|s$$

故

$$(ab)^s = e \Longrightarrow mn|s$$

命题14.7. 设G是有限$abel$群，G中一定有个元的阶是所有元的阶的倍数

这个命题的证明就是用前两个命题说明：对m阶元a和n阶元b，一定可以造一个元素$a^ib^j(i,j$适当取$)$，阶为$[a,b]$。

为了识别抽象的群，需要如下基本概念：

定义14.8. 设G_1，G_2是群。G_1到G_2的映射f称为一个同态，如果对任意$a,b \in G_1$,均有$f(ab) = f(a)f(b)$. 如果这个同态是双射，则称之为同构。如果存在这样一个同构，称G_1同构于G_2

例：下列三个群互相同构

$$(\mathbb{Z}/5\mathbb{Z})^\times, \quad \mathbb{Z}/4\mathbb{Z}, \quad U_4 = \{z \in \mathbb{C} | z^4 = 1\} = \{\pm 1, \pm i\}$$

把这三个群的元素按适当的顺序列出，依次对应可得需要的具体同构关系：

$\mathbb{Z}/4\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$

$(\mathbb{Z}/5\mathbb{Z})^\times = \{\overline{1}, \overline{3}, \overline{4}, \overline{2}\}$

$U_4 = \{1, i, -1, -i\}$

看一个简单的群论定理

定理14.9. 四个元素的群（叫四阶群）只有两个同构类。即可以给出两个不同构的四阶群，任何四阶群都同构于两者之一。

这个定理的证明留作练习，通过它可看出群论定理的味道。我们可以数论地给出这两个群

$$\mathbb{Z}/4\mathbb{Z}, \quad (\mathbb{Z}/8\mathbb{Z})^\times$$

粗略地说：抽象代数是研究抽象的群、环、域等代数对象；数论是研究具体的群、环、域等对象。

练习

1、验证三元集合$G = \{e, a, b\}$按下表定义的运算构成群

$$\begin{pmatrix} * & e & a & b \\ e & e & a & b \\ a & a & b & e \\ b & b & e & a \end{pmatrix}$$

并证明它同构于$\mathbb{Z}/3\mathbb{Z}$

2、证明开区间$A = (-1, +\infty)$按运算$a \circ b = a + b + ab$构成群，且同构于正实数的乘法群。

3、在群$\mathbb{Z}/15\mathbb{Z}$中以下元素的阶各是多少？

$\overline{3}, \overline{2}, \overline{10}$

4、在群$(\mathbb{Z}/35\mathbb{Z})^{\times}$中以下元素的阶各是多少？

$\overline{3}, \overline{2}$

5、证明适合左右消去律的有限半群一定是群。

15 子群

定义15.1. *如果群G有子集H，按照从G中继承的运算构成群，通常说H是G的子群，常记为$H < G$*

很显然，H能够称为子群需要满足下列两个条件：
(1) $a, b \in H \Longrightarrow ab \in H$
(2) $a \in H \Longrightarrow a^{-1} \in H$

(1)保证H能够继承G的运算，要使H能构成群，还需要(2)，事实上，这两条在一起就充分了，因为由这两条能保证

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

（剩下就好验证了）。把这两条结合起来可变成一条，即有下列命题。

命题15.2. *如果群G有子集H，则H是子群当且仅当*
$a, b \in H \Longrightarrow ab^{-1} \in H$

证明：只需验证这个条件等价于前面的(1)和(2)。

例1、考察群$\mathbb{Z}$的子群，检查以下子集：
$H_1 = \{1, 2, 3, 4, 5\}$，$H_2 = 3\mathbb{N} = \{3x | x \in \mathbb{N}\}$，$H_3 = 3\mathbb{Z}$

H_1不是子群，因为(1)不满足；H_1也不是子群，因为(2)不满足；H_3是子群，因为(1)和(2)都满足，或者说满足命题3.2.3的条件。事实上，对任意整数n，$n\mathbb{Z}$都是$\mathbb{Z}$的子群，反过来也对。

例2、$\mathbb{Z}$的子群一定是$n\mathbb{Z}$

证明，设$H < \mathbb{Z}$，若$H \neq \{0\}$，则H中有正数（$a \in H \Longrightarrow -a \in H$），取$n$为$H$中的最小正整数，断言

$$H = n\mathbb{Z}$$

首先H是子群就保证了$H \supset n\mathbb{Z}$，如果反包含不成立，即有$a \in H, a \notin n\mathbb{Z}$，用$a$对$n$做带余除法可得矛盾。

现举几个同态的例子：对群$\mathbb{Z}/15\mathbb{Z}$和$\mathbb{Z}/5\mathbb{Z}$，我们可以做两个同态

$$\phi : \mathbb{Z}/15\mathbb{Z} \longrightarrow \mathbb{Z}/5\mathbb{Z}$$

$$\overline{a} \bmod 15 \longmapsto \overline{a} \bmod 5$$

这是个良定义的映射，因为

$$\overline{a} \bmod 15 = \overline{b} \bmod 15 \Longrightarrow \overline{a} \bmod 5 = \overline{b} \bmod 5$$

是同态就好检查了。

$$\psi : \mathbb{Z}/5\mathbb{Z} \longrightarrow \mathbb{Z}/15\mathbb{Z}$$

$$\overline{a} \bmod 5 \longmapsto \overline{3a} \bmod 15$$

这是个良定义的映射，因为

$$\overline{a} \bmod 5 = \overline{b} \bmod 5 \Longrightarrow \overline{3a} \bmod 15 = \overline{3b} \bmod 15$$

是同态就好检查了。

进一步，由于ϕ是满射（显然），可称ϕ是满同态，类似地，由于ψ是单射（自己检查），可称ψ是单同态。

从以上子群的例子可以总结出，对群G中的任意元a，有子群

$$\langle a\rangle := \{a^n | n \in \mathbb{Z}\}$$

它是含有元a的最小（G的）子群，称为由a生成的子群。子群$\langle a\rangle$有限当且仅当a的阶有限，并且有

$$\text{子群}\langle a\rangle\text{的阶} = \text{元素}a\text{的阶}$$

进一步可验证（练习）：
若a的阶无限，则

$$\langle a\rangle \cong \mathbb{Z}$$

若a的阶是有限数r，则

$$\langle a\rangle \cong \mathbb{Z}/r\mathbb{Z}$$

定义15.3. 形如$\langle a\rangle = \{a^n | n \in \mathbb{Z}\}$的群称为循环群，把$a$称为该循环群的生成元（之一）。

对群G的子群H和元素$a \in G$，集合$aH = \{ah | h \in H\}$称为一个左陪集，同样可定义右陪集。

命题15.4. 如果群G有子群H，则$aH \neq bH \iff aH$与bH不交

证明：若$x \in aH \bigcap bH$，则存在$h_1, h_2 \in H$，满足$x = ah_1 = bh_2$，于是$a = bh_2h_1^{-1} = bh, h \in H$，这样

$$aH = b(hH) = bH$$

结合$G = \bigcup\limits_{a\in G} aH$有如下推论，即所谓拉格朗日定理。

定理15.5. G是有限群，H是G的子群，则H的阶整除G的阶

证明：因为群有消去律，可知H与aH之间存在双射，$h \longmapsto ah$，故$|H| = |aH|$。取S为G的满足以下条件的子集：
1) $a, b \in S, a \neq b \Longrightarrow aH \neq bH$
2) 对任意$a \in G$，存在$b \in S$，满足$aH = bH$
（当G=$\mathbb{Z}$，$H = n\mathbb{Z}$时，S是模n的一个完全剩余系）。由

$$G = \bigcup_{a\in G} aH = \bigcup_{a\in S} aH$$

看出$|G| = |H||S|$，当然$|H|$整除G.

特别地，（作为练习）可以有：对有限群G，元素的阶整除群G的阶。因为对任意$a \in G$，可给出一个G的循环子群$\langle a\rangle$，这个子群的阶恰好是a的阶。

练习：
1、证明素数阶群一定是循环群。对n阶循环群，请问几个元可充当它的生成元。
2、证明对群同态$\phi : G_1 \longrightarrow G_2$，有
(1) $\phi(e_1) = e_2$，
(2) $\phi(a^{-1}) = \phi(a)^{-1}$，
(3) 完全像$\phi(G_1)$是G_2的子群，

(4) 若ϕ单，则完全像$\phi(G_1)$与G_1同构

3、做出从群$\mathbb{Z}/5\mathbb{Z}$到群$\mathbb{Z}/15\mathbb{Z}$的所有同态。

4、做出从群$\mathbb{Z}/5\mathbb{Z}$到群$\mathbb{Z}/8\mathbb{Z}$的所有同态。

5、做出从群$\mathbb{Z}/5\mathbb{Z}$到自己的所有同态。

（提示：第3–5题的共同特点是任一同态ϕ由$\phi(\overline{1})$决定）

16 同态基本定理

定义16.1. 群G的子群H称为正规子群，记为$H \triangleleft G$，如果满足对任意$a \in G$，有$aH = Ha$

命题16.2. 设G是群，$H < G$，则以下几条等价

(1) H是正规子群

(2) 对任意$a \in G$有$aHa^{-1} = H$

(3) 对任意$a \in G$有$aHa^{-1} \subset H$

(4) 对任意$a \in G$有$aHa^{-1} \supset H$

对群G的子集A和B，引入记号（约定）

$$AB = \{ab | a \in A, b \in B\}$$

自然也有结合律

$$(AB)C = A(BC)$$

如果群运算记为加法，则有类似记号$A + B$。

对正规子群$H \triangleleft G$和任意陪集aH, bH，有

$$(aH)(bH) = a(Hb)H = a(bH)H = (ab)(HH) = abH \qquad *$$

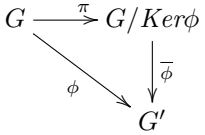
于是有以下概念：

定义16.3. 设群G有正规子群H，在集合$G/H = \{aH | a \in G\}$中定义运算$(aH)(bH) = abH$，然后G/H成为一个群，称为G对H的商群（*式保证了运算的合理性）。

注:一般地，$aH = Ha$并不意味着$ah = ha$对每个$h \in H$成立。当然若G是abel的，则任何子群都是正规的，因此可以做商群。例如：$\mathbb{Z}$对$n\mathbb{Z}$做商得$\mathbb{Z}/n\mathbb{Z}$.

例：集合$\{1, 2, 3\}$到自己的全部双射构成群（记为S_3），它有2阶和3阶子群，其中3阶子群（只有一个）是正规的，但2阶子群就不是。

定理16.4. （同态基本定理）设有群同态$\phi : G \longrightarrow G'$，称$Ker\phi := \{x \in G | \phi(x) = e'\}$为$\phi$的核。则$Ker\phi \triangleleft G$，且有如下交换图



并且$\overline{\phi}$是单同态。特别地，若ϕ是满的，则$\overline{\phi}$是同构。

证明：先证Ker$\phi \triangleleft G$，对任意$a \in G, x \in$ Kerϕ，有

$$\phi(axa^{-1}) = \phi(a)\phi(x)\phi(a)^{-1} = \phi(a)e'\phi(a)^{-1} = e'$$

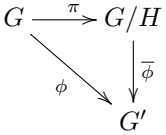
从而$axa^{-1} \in \mathrm{Ker}\phi$，说明$\mathrm{Ker}\phi \triangleleft G$。再证明由相同像给出的（$G$上的）等价关系与由陪集给出的等价关系一致，即

$$\phi(x) = \phi(a) \Longleftrightarrow xH = aH$$

（细节略去。对比线性方程理论中通解和特解的关系。）最后机械地验证$\overline{\phi}$的确是同态。

注：同态基本定理有以下常见的加细。

1) 若$H \triangleleft G$，则群同态$\phi : G \longrightarrow G'$有类似分解图



当且仅当$H < \mathrm{Ker}\phi$，进一步，只有在$H < \mathrm{Ker}\phi$时，$\overline{\phi}$ 是单的。

2) 若$K \triangleleft G'$，则$\phi^{-1}(K) \triangleleft G$。这只需对复合同态$G \longrightarrow G' \longrightarrow G'/K$用同态基本定理即可。

用同态基本定理，我们重新研究循环群：设有循环群$G = \{a^n | n \in \mathbb{Z}\}$，做同态

$$\phi : \mathbb{Z} \longrightarrow G$$

$$\phi(n) = a^n$$

它当然是同态，且是满的。由同态基本定理，有

$$\mathbb{Z}/ \cong \mathrm{Ker}\phi \cong G$$

当a是无限阶（即G是无限阶）时，$\mathrm{Ker}\phi = \{0\}$，此时

$$\mathbb{Z} \cong G,$$

当a是有限阶r时，$\mathrm{Ker}\phi = r\mathbb{Z}$，此时

$$\mathbb{Z}/r\mathbb{Z} \cong G$$

现在我们可证明定理3.2.9，即分类所有4阶群。设G是4阶群，由拉格朗日定理知G中元素的阶只能是1，2或4 1阶元就是单位元，另外3个元的阶是2或4，分两类：

(1) 存在一个4阶元a，则$G =$由a生成的群，即G是4阶循环群，$G \cong \mathbb{Z}/4\mathbb{Z}$

(2) G中所有非单位元都是2阶，设$G = \{e, a, b, c\}$，则

$$a^2 = b^2 = c^2 = e, ab = ba = c, ac = ca = b, bc = cb = a$$

这样的群在同构意义下是确定的，它同构于$(\mathbb{Z}/8\mathbb{Z})^\times$

与循环群（形式上）类似，我们可对群G的子集S，可考察包含S的最小子群，只要取包含S的所有子群的交（见练习2）。称这个子群为由S生成的子群，记为$\langle S\rangle$。如果记$S^{-1} = \{s^{-1} | s \in S\}$，则容易检查

$$\langle S\rangle = \{a_1 \cdots a_m | a_i \in S \cup S^{-1}, m > 0\}$$

练习。

1、设G是群，$H_i, i \in I$是一族G的子群，证明$\bigcap\limits_{i\in I} H_i$也是子群。

2、设G是群，A, B是G的子群，证明

1) AB是子群当且仅当$AB = BA$.

2) 若$A \triangleleft G$，则AB是子群。

3) $A \cup B$是子群当且仅当A和B有包含关系。

4) 若A, B都是有限的，则

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

3、考察由集合$\{1, 2, 3\}$到自己的所有双射按映射的合成构成的群S_3，将其中的元素

$1 \longmapsto i, 2 \longmapsto j, 3 \longmapsto k$

记为

$$\begin{pmatrix} 1 & 2 & 3 \\ i & j & k \end{pmatrix}$$

1) 列出所有元素并指出它的阶。

2) 找一个二元集合，使它能生成S_3.

3) 找出所有正规子群。

17 变换群

尽管数论中有大量的群，但群的概念在历史上来源于几何，可以说对称即群。

定义17.1. 对任意集合X，可定义$S(X)=\{X到自身的所有双射\}$按映射的合成形成群，称为X的全变换群，它的任意子群称为变换群。

我们将看到抽象群与变换群是一样的。

定理17.2. （*Cayley*）任何群都同构于一个变换群。

证明：设G是一个群，考察变换群$S(G)$。作映射
$\phi: G \longrightarrow S(G)$，$\phi(g)$定义为$G$到自己的左平移映射：$x \longmapsto gx$。首先由$G$是群知道$\phi(g)$的确在$S(G)$中，即$\phi$是映射。只要证明$\phi$是单同态即可。
1) 验证ϕ是同态。即证明对$a,b\in G$，有$\phi(ab)=\phi(a)\circ\phi(b)$，即证明对任意$x\in G$有

$$\phi(ab)(x)=(\phi(a)\circ\phi(b))(x)$$

而上式两端都是abx，当然相等。
2) 验证ϕ是单的，即由$\phi(a)=\phi(b)$导出$a=b$，而这是显然的，因为$a=\phi(a)(e)=\phi(b)(e)=b$。

对集合$X=\{1,2,...,n\}$，将$S(X)$简单记为S_n，称为n元对称群，群中的元素称为一个置换。显然任意含有n个元的集合X，相应的$S(X)$都同构。Cayley定理意味着群S_n很重要，因为它的子群包括了所有有限群。现在简单研究S_n，先看以下概念：
•**轮换** S_n中元素$(i_1...i_s)$：将i_1映到i_2，i_2映到i_3，以此类推，最后i_s映到i_1，保持其它的元不变。这个置换称为一个s-轮换。
•**对换** 两个元组成的轮换(ij)。
•**不动点** $\sigma\in S_n$的不动点指的是满足$\sigma(x)=x$的x。

基本性质：
1. 任何置换都可表为有限个对换之积。
2. 两个不相交的轮换必可交换；任意置换都可唯一地（不计顺序）表为不交的轮换之积。
3. s-轮换的阶为s.

现在可将以前见过的有限群实现为S_n的子群。
$\mathbb{Z}/4\mathbb{Z}$同构于S_4中由(1234)生成的子群；$(\mathbb{Z}/8\mathbb{Z})^\times$同构于$S_4$中由$(12)$和$(34)$生成的子群，即
$\{(1),(12),(34),(12)(34)\}$

18 平面图形的对称群

在常见的对称的几何图形比如长方形、正方形和圆中，怎样比较对称性的优劣？直观上看是圆最好，正方形次之，最差是长方形。对一般的平面图形$X\subset\mathbb{R}^2$，可以用一个群表示它的对称性，而这个群符合我们的直观。首先，图形的对称体现在该图形可以做某些运动而整体图形不变。什么是平面的运动？应该平面$\mathbb{R}^2$到自己的特殊的双射（即群$S(\mathbb{R}^2)$的特殊元素），它应该不改变图形的内部结构，当然应该是以下三类映射以及它们的合成：
平移、旋转和对折。

总结为群的语言就是平面$\mathbb{R}^2$的对称群$T(\mathbb{R}^2)$是群$S(\mathbb{R}^2)$的由平移、旋转和对折生成的子群。那么X的对称群$T(X)$是

$$\{\sigma \in T(\mathbb{R}^2 | \sigma(X) \subset X\}$$

现在总结一些新旧的群

例1、有限群$\mathbb{Z}/n\mathbb{Z}$，$(\mathbb{Z}/n\mathbb{Z})^\times$.

这些都是abel群。前者是循环群，后者只对特殊的n是循环群（何时循环是数论的下一个主要任务）。

例2、Clein群$\{e, a, b, c\}$，a, b, c均是2阶元，而且它们中任两个之积等于另一个，它同构于$(\mathbb{Z}/8\mathbb{Z})^\times$，也同构于长方形的对称群。

例3、二面体群$D_n := \{a^i b^j | i = 0, 1; j = 0, 1, ..., n-1\}$，其中$a$是2阶元，$b$是$n$阶元，且$b^j a = ab^{n-j}$，它同构于正$n$边行的对称群

例4、n元集$\{1, 2, ..., n\}$的对称群S_n。Cayley定理保证S_n及其子群包括了所有有限群。

例5、无限群加群$\mathbb{Z}$，$\mathbb{Q}$，$\mathbb{R}$，$\mathbb{C}$；及乘法群$\mathbb{Q}^*$，$\mathbb{R}^*$，$\mathbb{C}^*$。

这些群都交换，推广得到更一般的群

$\mathrm{GL}_n k$（一般线性群），k可取$\mathbb{Q}$，$\mathbb{R}$，$\mathbb{C}$等。它有子群$\mathrm{SL}_n k$(特殊线性群)也有$\mathrm{GL}_n\mathbb{Z}, \mathrm{SL}_n\mathbb{Z}$。$GL_n\mathbb{R}$还有其它重要的子群，比如正交群$O_n\mathbb{R}$（反映Eulcid空间的对称性）和特殊正交群$\mathrm{SO}_n\mathbb{R}$。特别地，$\mathrm{SO}_2\mathbb{R}$代表平面的旋转。

例7、集合$A = (-1, +\infty)$按运算$a \oplus b = a + b + ab$形成一个群，单位元是0，进一步这个群同构于正实数集$\mathbb{R}^+$按普通乘法构成的群。即有

$$\phi : A \longrightarrow \mathbb{R}^+$$

$$\phi(x) = x + 1$$

这个群有以下简单实用背景：

一个数上涨百分比a，再上涨百分比b，则上涨百分比$a \oplus b$。另外还可以证明正数的算术平均和几何平均的关系：

定理I：设$a_1, ..., a_n$是不全相等的正数，则

$$\frac{a_1 + \cdots + a_n}{n} > \sqrt[n]{a_1 \cdots a_n}$$

先用群A的语言将定理翻译如下

定理II：设$\varepsilon_1, ..., \varepsilon_n$是$A$中不全为0的元，则

$$\varepsilon_1 + \cdots + \varepsilon_n = 0 \Longrightarrow \varepsilon_1 \oplus \cdots \oplus \varepsilon_n < 0$$

翻译理由简述如下，取一个正数a，让它和那组数的算术平均和几何平均进行大小比较。令$\varepsilon_i = \frac{a_i - a}{a}$，那么

算术平均与a的大小比较就是$\varepsilon_1 + \cdots + \varepsilon_n$与0的比较；

几何平均与a的大小比较就是$\varepsilon_1 \oplus \cdots \oplus \varepsilon_n$与0的比较；

定理II的证明依据群A的以下简单事实：

1) a, b异号$\Longrightarrow a \oplus b < a + b$

2) $a_1 < a_2 \Longrightarrow a_1 \oplus b < a_2 \oplus b$

练习

1、证明对两个（可简单推广成有限个）不相交的轮换，它们的积的阶等于阶的最小公倍数。

2、对一般有限群G，若有$a, b \in G$和$ab = ba$，上述结论成立吗？以前只知道当阶互素时成立。

3、验证性质2。

4、群S_{10}中阶最大的元有多少个？是多少阶？

5、找出群D_n的所有2阶元并指出其几何意义（当看作正多边形的对称群时）。

19 环和域的基础知识

现列出环的有关概念。

• **环**：带有两个运算加法和乘法的集合R，R关于加法成交换群，关于乘法成幺半群（monoid），且乘法对加法有分配律。通常用0和1记加法和乘法单位元。

注记 有些书中的环可以没有乘法单位元1. 但本课程中的环都是有1的，当我们偶尔需用到没有1的环时，我们说R是一“不带1的环”。环也可能只含有一个元素，此时$1=0$，我们称这样的环为0环。

• **环同态**－两个环之间的映射，它保持运算和乘法单位元1.

注记－保持1这个要求并非多余的，例子见后面的练习：

• **子环**－环R的一个子环是指R的一个子集，它关于R的运算和乘法单位元构成环。

理想－环R的一个子加群I，如果满足

$$a\in R, b\in I \Longrightarrow ab\in I$$

称I为R的左理想，类似地可定义右理想。如果I既是左理想又是右理想，则称为双边理想或称理想。

注记 一般地，理想不是子环，子环不是理想。只能对理想作商环。对任意（非0）环，都有两个平凡理想，一个是最大的，即环本身；一个是最小的，即只含0的理想，我们称之为0理想。

• **商环**－设R是环，I是R的理想，则加法商群$R/I=\{a+I|a\in R\}$中再定义$(a+I)(b+I)=ab+I$，可得到一个环，称为R对I的商环，仍记为R/I. 通常记$\overline{a}=a+I$.

注记 乘法运算的合理性（即不依赖于代表元的选取）需证明，留作练习从R到商环R/I有自然同态$a\longmapsto\overline{a}$.

•**交换环（commutative ring），除环（division ring），域(field)** 对一个环R，若乘法交换，则称R为交换环；若非0元之集R^*构成乘法群，则称R为除环;交换的除环称为域。

注记 对交换环R，理想的最典型的例子是$aR:=\{ar|r\in R\}$，即某个元$a\in R$的所有倍元之集，我们称之为由a生成的主理想；一个非0交换环是域等价于它没有非平凡理想。大家作为练习去证明，并仔细体会。

• **理想的表示法**：对**交换环**R，有常见的理想如下

$$(a_1,...,a_n):=a_1R+\cdots+a_nR=\{a_1x_1+\cdots+a_nx_n|x_i\in R\},\ \text{称为由元素}a_1,...a_n\text{生成的理想}$$

$$(S)=\{a_1x_1+\cdots+a_nx_n|a_i\in S,x_i\in R\},\ \text{由子集}S\text{生成的理想}$$

•**整环**：交换环且有性质

$$ab=0\Longrightarrow a=0\text{或}b=0$$

•**单位群**：环R中的一个元a称为可逆元或单位，如果存在$b \in R$满足$ab = ba = 1$（b称为a的逆元，记为a^{-1}）；R中所有单位构成群，称为R的单位群，记为$R^\times$

20 环的例子

最基本的环是$\mathbb{Z}$，它是整环，不是域。还有$\mathbb{Q}, \mathbb{R}, \mathbb{C}$等常见的例子，这几个都是域，在高等代数这门课中提到数域，其实，那就是复数域的子域，而建立在数域上的线性空间理论都对任何抽象的域仍然成立。在数论中见过的环还有$\mathbb{Z}/n\mathbb{Z}$，它是整环当且仅当n为素数或0；它是域当且仅当n为素数。下面看几个其它例子：

1 对交换环R，R上全体n阶方阵构成环$\mathrm{M}_n(R)$，它一般是非交换的（只要$n > 1$）. 可定义矩阵$A \in \mathrm{M}_n(R)$的行列式$\det A$，且有如下基本结论：

矩阵可逆当且仅当行列式可逆。

R上n阶可逆矩阵形成乘法群，记为$\mathrm{GL}_(n, R)$。

2 现在给一个非交换的除环的例子，称为Hamilton四元代数，它是实数域的4维线性空间，又是一个除环，但不交换

第一种（抽象）定义：设有i, j, k三个符号，满足

$$i^2 = j^2 = k^2 = -1$$

和

$$ij = k = -ji, jk = i = -kj, ki = j = -ik,$$

记H为所有形如$a_1 + a_2 i + a_2 j + a_3 k$, $a_i \in \mathbb{R}$的对象的集合，在H上定义加法和乘法运算（上两组关系结合规定：$\mathbb{R}$中的元可与H中任何元交换可决定唯一的乘法运算）使之成为环。称H为Hamilton四元代数。可以验证H确实是除环。

第二种（具体）定义：在矩阵代数$\mathrm{M}_2(\mathbb{C})$中取由形如

$$\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}$$

的元素组成的$\mathbb{R}$-子空间H，显然它作为$\mathbb{R}$-空间是4维的，也容易验证它是子环（只需检查运算封闭）。它的一组自然的基为

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

将第一个矩阵视为1，其余3个分别视为第一种的i, j, k，显然满足那几组基本关系。

注记 两种定义的等价性很容易证明，第一种初看起来不易接受，但容易得到唯一性；第二种的存在性不需担心。实际上在H中与i, j, k具有同等地位的元素很多。H的任意包含$\mathbb{R}$的二维子空间一定构成一个子域且同构于复数域。对四元代数H上的元，可定义共轭元；利用共轭可定义从H到R有两个重要映射分别称为迹映射和范映射，细节见后边的练习。

3 多项式环和幂级数环

设R为交换环，可按通常运算定义R上的多项式环$R[X]$和形式幂级数环$R[[X]]$如下：

$$R[X] = \{\sum_{i=1}^{n} a_i X^i | n \in \mathbb{Z}, a_i \in R\}$$

$$R[[X]] = \{\sum_{i=1}^{\infty} a_i X^i | a_i \in R\}$$

注意X只是一个字母，与R无关。当然X也是$R[X]$和$R[[X]]$中的元素。定义另外两个环：A为R上序列之集按卷积运算构成的环，B为A的子环，由那些几乎所有项都为0的序列组成。显然有

$$A \cong R[[X]], B \cong R[X],$$

X对应于序列$0, 1, 0, 0, ...$。一个多项式f自然给出R到R的一个多项式函数，但多项式环和多项式函数环未必同构。多项式环据有如下范性：

设ϕ是从交换环R到任一交换环A的同态，则ϕ可自由地扩充到$R[X]$，只要任取$a \in A$，让$\phi(X) = a$即可。

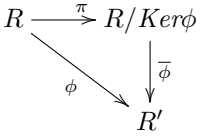
这个结论也可简单推广到多元多项式环。关于幂级数环有如下基本性质：

$\sum_{i=1}^{\infty} a_i X^i \in R[[X]]$**可逆当且仅当**$a_0$**可逆。**

21 基本定理

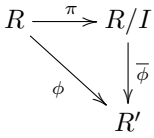
环也有同态基本定理

定理21.1. （同态基本定理）设有环同态$\phi : R \longrightarrow R'$，称$Ker\phi := \{x \in R | \phi(x) = 0\}$为$\phi$的核。则$Ker\phi$是$R$的理想，且有如下交换图



并且$\overline{\phi}$是单同态。特别地，若ϕ是满的，则$\overline{\phi}$是同构。

注：环同态基本定理也有以下常见的加细。
若I是R，则环同态$\phi : R \longrightarrow R'$有类似分解图



当且仅当$I \subset \mathrm{Ker}\phi$，进一步，只有在$I = \mathrm{Ker}\phi$时，$\overline{\phi}$ 是单的。

定理21.2. （拉格朗日定理）设F是域，则F上任意非零多项式的根的数目不超过多项式的次数。

高等代数中讲过F是数域的情形，前面讲过F为$\mathbb{Z}/p\mathbb{Z}$的情形，与一般情形的证明完全一样，不过是多项式环$F[X]$的唯一分解性的简单应用。

回顾$\mathbb{Z}$和$F[X]$的唯一分解定理的证明的注意思想，关键是利用带余除法得到基本性质：

设R是$\mathbb{Z}$或$F[X]$，对任意$a,b\in R$，存在$u,v\in R$使得

$$au+bv=(a,b)$$

这个性质的证明可以分为三部：
(1) 集合$aR+bR$是R的理想（以前没有理想这个名词）；
(2) 利用带余乘法证明R的理想一定具有形状dR，这个d是理想中最“小”的元（之一），在$\mathbb{Z}$中，“小”指的绝对值小；在$F[X]$中，“小”指的次数小。
(3) 由前两步得$aR+bR=dR$，进而推出d是a,b的最大公因子，因为这个等式告诉你：
1) $dR\supset aR,bR$，从而$d|a,d|b$
2) $x|a,x|b\Longrightarrow x|d$

22 环、域与数论

可以相信环的单位群特别是域的乘法群一定是很特殊的群，原始的Wilson定理就是利用域$\mathbb{Z}/p\mathbb{Z}$的乘法群只有一个2阶元-1，因为在域上方程

$$x^2=1$$

只能解出$x=\pm1$

由于在任意域上$x^n=1$只能有至多n个根，这个重要性质会导出以下基本定理

定理22.1. 域的乘法群的有限子群一定是循环群。

推论22.2. $(\mathbb{Z}/p\mathbb{Z})^*$是循环群。

定理的证明：设有域F，和F^*的n阶子群G，想找到G中一个n阶元：
方法一：由于对任意$a,b\in F^*$，总能找到适当的i,j使a^ib^j的阶达到a的阶与b的阶的最小公倍数，故

只要a的阶不是b的阶的倍数，则有某元a^ib^j的阶大于a的阶

换句话说，如果a是G中阶最大的元，则a的阶是所有（G中的）元的阶的倍数。记m为a的阶，那么对任意$x\in G$，有$x^m=1$，由域的拉格朗日定理知

$$|G|\leq m$$

由群的拉格朗日定理知$m||G|$. 所以$|G|=m$，即G是由a生成的循环群。
方法二：设$n=p_1^{r_1}\cdots p_m^{r_m}$，证明$G$中有元$a_i$阶为$p_i^{r_i}$即可（$a_1\cdots a_m$的阶为$n$），阶为$p_i^{r_i}$的元即是满足下列条件

$$x^{p_i^{r_i}}=1,x^{p_i^{r_i-1}}\neq1$$

因此只需说明方程$x^{p_i^{r_i}}=1$的解数多于方程$x^{p_i^{r_i-1}}=1$的解数。这是对的，因为两个方程的解数都正好是各自的次数，这又是因为一方面，

“方程$x^n=1$的解数恰为次数n（G中所有元）”

另一方面，有多项式关系$X^{p_i^{r_i}}-1|X^n-1$。
方法三：证明只要群F^*中有d阶元a，则方程$x^d=1$在F^*中恰有d个解（a生成的循环子群），于是可数出全体d阶元个数为$\phi(d)$，将G按元素的阶分类，记G_d为G中所有d阶元之集，则

$$G=\cup_{d|n}G_d$$

于是

$$n=\sum_{d|n}|G_d|$$

这个等式结合前面讨论知道每个G_d不空。细节留作练习。

练习

1、证明任意整环上非0多项式的根的数目不超过次数。

2、在环$\mathbb{Z}/100\mathbb{Z}$上写出多项式X^2-X的各种可能的分解。

3、设F是域，F上任意一个多项式f可自然地给出一个F到F的函数，把这种函数称为多项式函数，定义两个函数的加法和乘法（函数值相加和相乘），全体多项式函数形成一个环。利用同态基本定理证明：

(1) 如果F是无限域，则多项式函数环同构于多项式环；

(2) 如果$F=\mathbb{Z}/p\mathbb{Z}$，则多项式函数环同构于$F[X]/(X^p-X)$

4、有拉格朗日定理证明域的乘法群里如果有d阶元，则恰好有$\phi(d)$个。

5、利用上题的结论证明定理2.10.1

（提示将给定的有限乘法群的元素按阶分类并数数）

6、证明任何环同态一定将单位应到单位。

7、对环R_1,R_2，在笛卡尔乘积$R_1\times R_2$上定义自然的运算（分量分别运算），证明$R_1\times R_2$也构成环，且

(1) $(R_1\times R_2)^\times=R_1^\times\times R_2^\times$

(2) 对两个互素的整数m,n，有

$$\mathbb{Z}/(mn)\cong\mathbb{Z}/(m)\times\mathbb{Z}/(n)$$

8、设G为n阶交换群，证明以下三条等价：

(1) G为n阶循环群

(2) 对任意$d|n$，方程$x^d=1$的解数恰为d

(3) 对任意$d|n$，方程$x^d=1$的解数不超过d

原根和二次剩余

第八周 群$(\mathbb{Z}/m\mathbb{Z})^\times$

23 模素数幂的原根存在性

设有互素的整数a和m，称a是模m的原根，如果$a^i,i=1,...,\phi(m)$正好构成模m的一个剩余缩系。换句话说：群$(\mathbb{Z}/m\mathbb{Z})^\times$是循环群，以$\bar{a}$为生成元，简单说就是$a$模$m$的阶（群$(\mathbb{Z}/m\mathbb{Z})^\times$中元$\bar{a}$的阶）是$\phi(m)$。

一个基本问题是对什么m，原根存在？存在时如何判别和寻找？

我们已经知道模p的原根存在，其原因是$\mathbb{Z}/p\mathbb{Z}$是域。回顾以下命题

设有互素的整数a和m，那么a模m的阶是n的充分必要条件是
1) $a^n\equiv 1\pmod m$，
2) 对n的任一素因子q，有$a^{\frac{n}{q}}\not\equiv 1\pmod m$

它的特殊情形，我们有

设有互素的整数a和m，那么a是模m的原根的充分必要条件是:
对$\phi(m)$的任一素因子q，有$a^{\frac{\phi(m)}{q}}\not\equiv 1\pmod m$

例：3是模7的原根。因为$3^{\frac{6}{2}}\not\equiv 1\pmod 7, 3^{\frac{6}{3}}\not\equiv 1\pmod 7$

现在考察模p^l的情形：首先，当$p=2$时，模2^2的原根存在，但当$l>2$时，不存在模2^l的原根。因为对任意奇数a有

$$a^{2^{l-2}} \equiv 1 \pmod{2^l}$$

定理23.1. *若p为奇素数，$l>1$，a是一整数，则a是模p^l的原根当且仅当下列两条同时成立*
1) a是模p的原根;
2) $a^{p-1} \not\equiv 1 \pmod{p^2}$

注：这个定理暗含了对$l>1$，a是模p^l的原根等价于a是模p^2的原根。同时保证了模p^2的原根存在性，因为对满足1)的a总可取适当的t（$p-1$种取法）使得$a^{p-1} \not\equiv 1 \pmod{p^2}$。特别地$a$和$a+p$必有一个满足2)。为证明这个定理，先做一些准备

引理23.2. *设p为素数，n是正整数，则*

$$a \equiv b \pmod{p^n} \Longrightarrow a^p \equiv b^p \pmod{p^{n+1}}$$

这个引理的证明留作练习，用二项式定理即可。可以得出如下推论

推论23.3. *设p为素数，n是正整数，则*

$$a\text{是模}p^{n+1}\text{的原根} \Longrightarrow a\text{是模}p^n\text{的原根}$$

证明：若a不是模p^n的原根，则有正整数$r<\phi(p^n)$，满足

$$a^r \equiv 1 \pmod{p^n}$$

再由引理4.1.2知

$$a^{rp} \equiv 1 \pmod{p^{n+1}},$$

而$rp < p\phi(p^n) = \phi(p^{n+1})$，与$a$是模$p^{n+1}$的原根矛盾。

引理4.1.2的逆也几乎是对的

引理23.4. *设p为奇素数，n是正整数，则对与p互相素的整数a和b，有*

$$a^p \equiv b^p \pmod{p^{n+1}} \Longrightarrow a \equiv b \pmod{p^n}$$

证明：记$r=\mathrm{ord}_p(a-b)>0$，即$p^r||a-b$，可设

$$a = b + tp^r, t \not\equiv 0 \pmod{p}$$

$$a^p = (b+tp^r)^p \equiv b^p + tb^{p-1}p^{r+1} \pmod{p^{r+2}}$$

由于$tb^{p-1} \not\equiv 0 \pmod{p}$，上式意味着$p^{r+1}||a^p-b^p$。结合$a \equiv b \pmod{p^{n+1}}$知$r+1 \geq n+1$，即$r \geq n$.

定理证明：先证必要性：假设a是模p^n的原根，由推论已知道a是模p^2的原根，也是模p的原根，剩下条件2)，但这由a是模p^2的原根保证。再证充分性：要证a是模p^n的原根，即证对$\phi(p^n)=p^{n-1}(p-1)$的任一素因子q，均有

$$a^{\frac{p^{n-1}(p-1)}{q}} \not\equiv 1 \pmod{p^n} \qquad (*)$$

由于q只能是p或$p-1$的因子，分别讨论如下：
(1) 若$q|p-1$，
那么$a^{\frac{p-1}{q}} \not\equiv 1 \pmod{p}$，由Fermat小定理知$a^{\frac{p^{n-1}(p-1)}{q}} \not\equiv 1 \pmod{p}$，当然(*)式成立。

(2) 若$q=p$（此时自动有$n>1$），
由条件2)不断用引理4.1.4，得$a^{p^{n-2}(p-1)}\not\equiv 1 \pmod{p^n}$，即此时(*)式成立。

这个定理不仅给出了模奇素数幂的原根存在性，还给出了寻找原根的方法：先找模p的原根a，再检查条件2)，a和$a+p$中必有一个适合，那么它就是模p的任意方幂的原根。

例、求模25的原根。

解：先找模5的原根2，计算知$2^4\equiv 16\not\equiv 1 \pmod{25}$，故2是模25的原根，进一步，$2+5t$，$t=0,1,2,3,4$中恰有一个(7)不是模25的原根。

例、求满足$100|2^n+n^2$的所有正整数n。

解：分别考察$4|2^n+n^2$和$25|2^n+n^2$，前者很简单，就是要求n是正的偶数；后者换个写法为

$$-2^n\equiv n^2 \pmod{25}$$

由于2是模25的原根，因此左边不断地过模25的剩余缩系，当n不断地过模20的剩余系时；而右边只能取模25的平方元。由于$-2^n\equiv 2^{n+10} \pmod{25}$，因此

$$-2^n\equiv a^2 \pmod{25}(\text{对某个}a)\Longleftrightarrow 2|n+10\Longleftrightarrow 2|n$$

进一步

$$-2^n\equiv a^2 \pmod{25}\Longleftrightarrow n=2t,\text{且}a\equiv\pm 2^{t+5}$$

于是让t取1到10，分别解同于方程组

$$\begin{cases} n\equiv 2t \pmod{20} \\ n\equiv \pm 2^{t+5} \pmod{25} \end{cases}$$

即可得出全部所需，细节自己补上，顺便发现$4|2^n+n^2$这个条件被涵盖了。

24 模任意整数的乘法群

命题24.1. *$m_1,...,m_k$是两两互素的整数，整数a模m_i的阶是r_i，则a模$m_1\cdots m_k$的阶是$[r_1,...,r_k]$.*

证明：对任意n，有

$$a^n\equiv 1 \pmod{m_1\cdots m_k}\Longleftrightarrow a^n\equiv 1 \pmod{m_i}\text{对每个}i\text{成立}\Longleftrightarrow r_i|n\text{对每个}i\text{成立}\Longleftrightarrow [r_1,...,r_k]|n$$

故a模$m_1\cdots m_k$的阶是$[r_1,...,r_k]$。

推论24.2. *$m_1,...,m_k$是两两互素的整数，整数a是模$m_1\cdots m_k$的原根当且仅当对每个i，a是模m_i的原根，且每个$\phi(m_i)$两两互素。*

证：设a模m_i的阶是r_i，于是a模$m_1\cdots m_k$的阶是

$$[r_1,...,r_k]\le r_1\cdots r_k\le\phi(m_1)\cdots\phi(m_k)=\phi(m)$$

因此a是模$m_1\cdots m_k$的原根当且仅当$r_i=\phi(m_i)$，且两两互素。

定理24.3. *模m的原根存在当且仅当m是以下几类之一：2、4、p^l、$2p^l$.*

证：由推论易知必要性，简单检查结合定理4.1.1知充分性成立。

练习

1、详细解答例2，并回答，在10000以内有多少个解。

2、设p是素数，$a \not\equiv 0 \pmod{p}$，a模p^n的阶是r_n，证明：

1) 对任意$n > 0$，有$r_{n+1} = r_n$或pr_n

2) 存在正整数N，满足当$n \geq N$时$r_{n+1} = pr_n$，请问当n小时怎样？

3、设p是奇素数，$st = p - 1$，证明

$$a^s \equiv 1 \pmod{p} \Longleftrightarrow \text{存在}b\text{满足}a \equiv b^t$$

4、找一个模169的原根，和一个整数，它是模13的原根，但不是模169的原根。

5、找一个模$5^2 \times 13$的阶最大的元。

6、证明对$n > 2$，$(-1)^i \times 5^j$，$i = 0, 1, ..., j = 0, 1, ..., 2^{n-2} - 1$，组成一组模$2^n$的剩余缩系。是否有

$$(\mathbb{Z}/16\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$$

7、若a是模m的原根，那么模m的所有原根是什么？有多少？

25 高次剩余

命题25.1. 设p是奇素数，$st = p - 1$，则

$$a^s \equiv 1 \pmod{p} \Longleftrightarrow \text{存在}b\text{满足}a \equiv b^t \pmod{p}$$

证明一：首先$\Longleftarrow$是显然的；齐次由于满足两边条件的a（在模p意义下）都是有限的，我们只需数数即可：左边的a就是方程$x^s - 1 \equiv 0 \pmod{p}$的解，由于$x^s - 1 | x^{p-1} - 1$，故有$s$个解。满足右边的$a$也应是$\frac{p-1}{t} = s$，因为$t$次幂映射将$(\mathbb{Z}/p\mathbb{Z})^\times$中$t$个不同的元变成一个。这又是因为方程$x^t \equiv 1 \pmod{p}$的解数是$t$.

证明二：取一个原根g，建立群同构$\tau : \mathbb{Z}/(p-1)\mathbb{Z} \cong (\mathbb{Z}/p\mathbb{Z})^\times$

$\overline{i} \longmapsto \overline{g^i}$

通过这个同构τ，准确地说是τ^{-1}，将命题翻译为$\mathbb{Z}/(p-1)$中的问题如下：

$$sn \equiv 0 \pmod{p-1} \Longleftrightarrow \text{存在}m\text{满足}n \equiv tm$$

这是显然的。

26 指数

设g是模m的原根，$(a, m) = 1$，则存在唯一整数d，满足$0 \leq d < \phi(m)$和$g^d \equiv 1 \pmod{m}$，称d为a对g的指数（或离散对数），记为$\text{ind}_g a$，有时可简单记为$\text{ind}a$。于是有以下性质：

$$\text{ind}ab \equiv \text{ind}a + \text{ind}b \pmod{\phi(m)}$$

$$\text{ind}a^n \equiv n\text{ind}a \pmod{\phi(m)}$$

对$d|\phi(m)$，有a是模m的d次剩余当且仅当$d|\text{ind}a$，特别地对奇素数p，有：

a是模p的2次剩余当且仅当$2|\text{ind}a$

练习求模49的一个原根，并求ind2

27 公钥密码应用

现在简要介绍两种公钥密码体制：由公开的加密密钥不能在有效时间内算出解密密钥的密码体制。

1. RSA体制

取一个整数$m = pq$，p, q是不同的大素数，再取整数d，满足$(d, \phi(m)) = 1$。将信息翻译成m以内的正整数，按如下方法加密信息a，

$$f(a) = b \equiv a^d \pmod{pq},$$

解密方法是

$$a \equiv b^e \pmod{pq}$$

e由关系$de \equiv 1 \pmod{(p-1)(q-1)}$确定。

公开m和d，但保密p和q，这样其他人无法计算$\phi(m)$（除非他能分解m），因此无法得到解密密钥e。

因此RSA体制是建立在大数分解这一难题基础上。

2. 离散对数体制

对一个大的素数p，和给定的原根g，计算ind$a$也没有快速算法，但计算$x^n \bmod p$却有快速算法，基于此有下列公钥密码体制：

公开p，g，和$a \equiv g^r \pmod{p}$，r很大。

保密r。

加密方案：甲方（不知r，只知a）要向乙方发送信息x（某一小于$\frac{p}{2}$的整数）。先取一大的随机数n，计算$g^n \equiv b \pmod{p}$和$a^n x \equiv y \pmod{p}$，然后发送数组(b, y)

解密方法：利用关系$b^r x \equiv y \pmod{p}$可算出x。

由于只有乙方知道r，故只有乙方才能解密。当然若某人有计算离散对数的快速算法，他就可破译。

注：这里只是简单介绍了数学原理，实际使用中有些变化。但这类基于数学（计算）难题的公钥密码体制的确已经使用，而且带来了方便。因为发放密钥更方便，甚至不需要通信双方是朋友关系。深刻的现代数论也不断地在密码领域找到应用。

28 原根判别举例

例1、判别2是否模13的原根。

解：$2^{\frac{12}{2}} \equiv -1 \not\equiv 1 \pmod{13}, 2^{\frac{12}{3}} \equiv 3 \not\equiv 1 \pmod{13}$. 故2是模13的原根。

例2、判别3、5是否模23的原根。解：$5^{\frac{22}{2}} \equiv -1 \not\equiv 1 \pmod{23}, 5^{\frac{22}{11}} \equiv 2 \not\equiv 1 \pmod{23}$. 故5是模23的原根。但$3^{\frac{22}{2}} \equiv 1 \pmod{23}$. 故3不是模23的原根。

例1的计算很容易，例2中计算$a^{\frac{p-1}{2}} \bmod p$时复杂得多，我们将看到这会有简单的算法。

第九周 二次互反律

29 二次剩余

定义29.1. *设有奇素数p，与p互素的a称为模p的二次剩余，如果方程$x^2 \equiv a \pmod{p}$有解，这就是前面讲的d次剩余取$d = 2$*

易知在一个缩系中，二次剩余和非二次剩余各占一半，而且

$$a\text{是二次剩余} \Longleftrightarrow a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

由于$a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$，故

$$a\text{是非二次剩余} \Longleftrightarrow a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

定义29.2. $(\frac{\cdot}{p})$称为勒让德符号，

$$(\frac{a}{p}) = \begin{cases} 1, a\text{是二次剩余} \\ -1, \text{是非二次剩余} \end{cases}$$

由定义立得

$$(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

因此有

$$(\frac{ab}{p}) \equiv (\frac{a}{p})(\frac{b}{p}) \pmod{p}$$

$$(\frac{-1}{p}) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$$

由于上两式的两端取值都是± 1，而$p > 2$，因此同余式变成等式。总结基本性质如下:

(1) $(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \pmod{p}$

(2) $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$

(3) $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$

经过一点计算可得另一基本性质：

(4) $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$

通过以上(2),(3),(4)条性质还不足以计算任意勒让德符号，还需要如下重要的二次互反律:

(5) 对不同的奇素数p和q，有

$$(\frac{q}{p})(\frac{p}{q}) = (-1)^{(\frac{p-1}{2})(\frac{q-1}{2})}$$

或等价地说成

$$(\frac{q}{p}) = \begin{cases} (\frac{p}{q}), p \equiv 1 \pmod{4} \text{或} q \equiv 1 \pmod{4} \\ -(\frac{p}{q}), p \equiv q \equiv 3 \pmod{4} \end{cases}$$

先不急于证明二次互反律，举个例子说明它的威力。

因为$(\frac{5}{353}) = (\frac{353}{5}) = (\frac{3}{5}) = -1$，故5是模353的非二次剩余。再算一个例子

$$(\frac{17}{41}) = (\frac{41}{17}) = (\frac{7}{17}) = (\frac{17}{7}) = (\frac{3}{7}) = -(\frac{7}{3}) = -(\frac{1}{3}) = 1$$

现在对具体$p = 13$，计算$(\frac{2}{13})$，从中可以看出计算一般的$(\frac{2}{p})$的方法，也包含证明二次互反律所需高斯引理的思想。

记$A = \{1, 2, 3, 4, 5, 6\}$，当然$A \bigcup (-A)$是一剩余缩系。$2A = 2, 4, 6, 8, 10, 12 \equiv \{2, 4, 6, -5, -3, -1\}$，因此

$$2^6(6!) = \prod_{i \in 2A} i \equiv (-1)^3(6!) \pmod{13}$$

故$2^6 \equiv -1 \pmod{13}$。这样$(\frac{2}{13}) = -1$

练习

1、用前面计算$(\frac{2}{13})$的方法推导一般的计算$(\frac{2}{p})$的公式。

2、推广前面的方法计算$(\frac{7}{23})$，并用二次互反律验算。
3、证明：群$(\mathbb{Z}/p\mathbb{Z})^\times$到群$\{\pm 1\}$的非平凡同态（即像不止取1）是唯一的，正是由勒让德符号给出的那个。

30 二次互反律的证明和应用

30.1 Gauss引理

我们来证明二次互反律，采用Gauss的初等证明，这需要一个关键的Gauss引理（不仅是结论，包括思想），而原始的思想正是来自计算$(\frac{2}{p})$的方法，让我们从前面计算$(\frac{2}{13})$的方法开始：

记$A=\{1,2,...,\frac{p-1}{2}\}$，模$p$有两个最简单的缩系。一是

$$\{1,2,...,p-1\}=A\bigcup(p-A);$$

一是

$$A\bigcup(-A).$$

考察$2A=\{x_1,...,x_n\}\bigcup\{y_1,...,y_m\}$，其中

$$\{x_1,...,x_n\}=2A\bigcap A,\{y_1,...,y_m\}=2A\bigcap(p-A)$$

同时因$2A\bigcup(-2A)$也是一组模p的缩系，说明$x_1,...,x_n,-y_1,...,-y_m$模$p$互不相同，故

$$A=\{x_1,...,x_n,p-y_1,...,p-y_m\}$$

于是

$$\prod_{i\in A}i\equiv(-1)^m x_1\cdots x_n y_1\cdots y_m$$

另一方面

$$2^{\frac{p-1}{2}}\prod_{i\in A}i=\prod_{i\in 2A}i=x_1\cdots x_n y_1\cdots y_m$$

综上两式知

$$2^{\frac{p-1}{2}}\equiv(-1)^m$$

即$(\frac{2}{p})=(-1)^m$。由m的定义:m是$2A$中$<\frac{p}{2}$的元的个数，即A中$>\frac{p}{4}$的元的个数，故$m=[\frac{p}{2}]-[\frac{p}{4}]\equiv\frac{p^2-1}{8}\pmod 2$，这样，

$$(\frac{2}{p})=(-1)^{\frac{p^2-1}{8}}\pmod p$$

注:称集合$A=\{a_1,...,a_{\frac{p-1}{2}}\}$为模$p$的一个半系，若$A\bigcup(-A)$是一剩余缩系。显然，对任意$a\not\equiv 0\pmod p$，$aA$仍是半系，因此$aa_i\equiv\varepsilon_i b_i\pmod p,\varepsilon_i=\pm1,b_1,...,b_{\frac{p-1}{2}}$为$a_1,...,a_{\frac{p-1}{2}}$的一个置换，考察$\prod_{i\in aA}i$可得$a^{\frac{p-1}{2}}\equiv\varepsilon_1\cdots\varepsilon_{\frac{p-1}{2}}\equiv(-1)^m$，这里$m$为$\varepsilon_1,...,\varepsilon_{\frac{p-1}{2}}$中$-1$的个数，即（在模$p$下）$aA$与$-A$交的数目。前面的计算就是用这一简单想法，总结起来就是如下Gauss引理

引理30.1. 设A为模p的一个半系，$a\not\equiv 0\pmod p$，$aA=\{x_1,...,x_n,y_1,...,y_m\}$，其中$\{x_1,...,x_n\}$同余于$A$的一个子集，$\{y_1,...,y_m\}$同余于$-A$的一个子集。则$(\frac{a}{p})=(-1)^m$

取$A=\{1,2,...,\frac{p-1}{2}\}$，得到如下特殊形式的Gauss引理

引理30.2. 设$a,2a,...,\frac{p-1}{2}a$这些数对p的最小非负剩余中$>\frac{p}{2}$的个数为m，则

$$(\frac{a}{p})=(-1)^m$$

再用例子$(\frac{3}{13})$说明Gauss引理：

$$A=\{1,2,3,4,5,6\}$$

$$3A=\{3,6,9,12,15,18\}\equiv 3,6,9,12,2,5\equiv 3,6,-4,-1,2,5$$

考察$\prod_{i\in 3A} i$可知

$$3^6\equiv(-1)^2=1 \pmod{13}$$

故$(\frac{3}{13})=1$。

30.2 二次互反律的证明

设p,q是不同的奇素数，我们用Gauss引理计算$(\frac{q}{p})$，依次对$q,2q,...,\frac{p-1}{2}q$做带余除法

$$kq=pq_k+r_k, 0<r_k<p$$

取

$$A=\{1,2,...,\frac{p-1}{2}\},$$

那么

$$qA\equiv\{r_1,...,r_{\frac{p-1}{2}}\}$$

记$A\bigcap\{r_1,...,r_{\frac{p-1}{2}}\}=\{x_1,...,x_n\}$，于是可设$\{r_1,...,r_{\frac{p-1}{2}}\}=\{x_1,...,x_n,y_1,...,y_m\}$（这里$x_i<\frac{p}{2}$，$y_j>\frac{p}{2}$）和$A=\{1,2,...,\frac{p-1}{2}\}=\{x_1,...,x_n,p-y_1,...,p-y_m\}$。求和有

$$\sum_{k=1}^{\frac{p-1}{2}} r_k=\sum_{i=1}^{n}x_i+\sum_{j=1}^{m}y_j \tag{1}$$

和

$$\sum_{k=1}^{\frac{p-1}{2}} k=\sum_{i=1}^{n}x_i+\sum_{j=1}^{m}(p-y_j) \tag{2}$$

在(1)中用$kq-pq_k$换r_k得

$$q\sum_{k=1}^{\frac{p-1}{2}}k-p\sum_{k=1}^{\frac{p-1}{2}}q_k=\sum_{i=1}^{n}x_i+\sum_{j=1}^{m}y_j \tag{3}$$

现通过(2),(3)两式得出m的信息，由于我们只关心m的奇偶性即$m \bmod 2$，故对两式取模2（注意到$p\equiv q\equiv 1 \pmod 2$）可得

$$m\equiv\sum_{k=1}^{\frac{p-1}{2}}q_k\equiv\sum_{k=1}^{\frac{p-1}{2}}[\frac{kq}{p}] \pmod 2$$

即

$$(\frac{q}{p})=(-1)^{\sum\limits_{k=1}^{\frac{p-1}{2}}[\frac{kq}{p}]}$$

，同理

$$(\frac{p}{q})=(-1)^{\sum\limits_{k=1}^{\frac{q-1}{2}}[\frac{kp}{q}]}$$

于是

$$(\frac{q}{p})(\frac{p}{q})=(-1)^{\sum\limits_{k=1}^{\frac{p-1}{2}}[\frac{kq}{p}]+\sum\limits_{k=1}^{\frac{q-1}{2}}[\frac{kp}{q}]}$$

剩下只需证

$$\sum_{k=1}^{\frac{p-1}{2}}[\frac{kq}{p}]+\sum_{k=1}^{\frac{q-1}{2}}[\frac{kp}{q}]=\frac{p-1}{2}\frac{q-1}{2} \tag{4}$$

这需要利用长方形$\{(x,y)|0<x<\frac{p}{2},0<y<\frac{q}{2}\}$。内部的整点数目是$\frac{p-1}{2}\frac{q-1}{2}$，沿对角线$y=\frac{q}{p}x$分成两个三角形内部的整点数目分别是$\sum_{k=1}^{\frac{p-1}{2}}[\frac{kq}{p}]$和$\sum_{k=1}^{\frac{q-1}{2}}[\frac{kp}{q}]$，而对角线上无整点，这就证明了(4)，从而证明了二次互反律。

30.3 应用举例

例1、判别3是否模23的原根。

解：$23-1=22$有两个素因子2和11

$$3^{22/11}=3^2\not\equiv 1 \pmod{23}$$

$$3^{22/2}\equiv(\frac{3}{23})=-(\frac{23}{3})=-(\frac{2}{3})=1 \pmod{23}$$

故3不是模23的原根。

例2、判别3是否模Fermat素数$p=2^n+1,n>1$的原根。

解：$(\frac{3}{p})=(\frac{p}{3})=(\frac{2}{3})=-1$

即$3^{\frac{p-1}{2}}\equiv -1 \pmod{p}$。由于$p-1$只有素因子2，故3是模$p$的原根。

例3、设$p=4q+1$，p、q都是素数，则2是模p的原根。

证明：$p-1$有两个素因子2和q，

$$2^{p-1/q}=16\not\equiv 1 \pmod{p}$$

（因为p不是3、5）

$$2^{p-1/2}\equiv(\frac{2}{p})=-1\not\equiv 1 \pmod{p}$$

（因为$q\equiv 1 \pmod 2 \Longrightarrow 2q+1\equiv 5 \pmod 8$）

因此2是原根。

例4、证明：对任意整数m,n，$\frac{4n^2+1}{m^2+2}$不是整数。

证明：设p是$4n^2+1$的任一素因子，则p奇，且$-1\equiv(2n)^2\equiv p$，即$(\frac{-1}{p})=1$，即$p\equiv 1 \pmod 4$。说明$4n^2+1$的任何因子都$\equiv 1 \pmod 4$，但$m^2+2\equiv 2,3 \pmod 4$。

例5、对什么素数p，3是二次剩余；对什么素数p，-3是二次剩余；

解：因$(\frac{3}{p})=(-1)^{\frac{p-1}{2}}(\frac{p}{3}$，故

$$(\frac{3}{p})=1\Longleftrightarrow\begin{cases}p\equiv 1 \pmod 4\\ p\equiv 1 \pmod 3\end{cases}\text{或}\begin{cases}p\equiv -1 \pmod 4\\ p\equiv -1 \pmod 3\end{cases}\Longleftrightarrow p\equiv\pm 1 \pmod{12}$$

因$(\frac{-3}{p})=(\frac{-1}{p})(-1)^{\frac{p-1}{2}}(\frac{p}{3})=(\frac{p}{3})$，故

$$(\frac{-3}{p})=1\Longleftrightarrow p\equiv frm[o]-- \pmod 3$$

对上式也可另证：

$$p \equiv 1 \pmod 3 \Longleftrightarrow \text{群}(\mathbb{Z}/p\mathbb{Z})^{\times}\text{有3阶元} \Longleftrightarrow x^3 - 1 \equiv 0 \pmod p\text{有1以外的解}$$

$$\Longleftrightarrow x^2 + x + 1 \equiv 0 \pmod p\text{有解} \Longleftrightarrow -3\text{在域}\mathbb{Z}/p\mathbb{Z}\text{上是平方元}$$

30.4 推广的二次互反律

定义30.3. 设$n = p_1^{l_1} \cdots p_r^{l_r}$为奇数，则可对与$n$互素的$m$定义*Jacobi*符号

$$(\frac{m}{n}) = (\frac{m}{p_1})^{l_1} \cdots (\frac{m}{p_r})^{l_r}$$

注: $(\frac{m}{n}) = -1$推出方程$x^2 \equiv m \pmod n$无解，但$(\frac{m}{n}) = 1$不能推出方程$x^2 \equiv m \pmod n$有解。

Jacobi符号具有勒让德符号的相应的性质，特别是二次互反律：

(1) 若$a \equiv b \pmod n$，则$(\frac{a}{n}) = (\frac{b}{n})$

(2) $(\frac{ab}{n}) = (\frac{a}{n})(\frac{b}{n})$

(3) $(\frac{-1}{n}) = (-1)^{\frac{n-1}{2}}$

(4) $(\frac{2}{n}) = (-1)^{\frac{n^2-1}{8}}$

(5) 推广的二次互反律。对互素的奇数m和n，有

$$(\frac{m}{n})(\frac{n}{m}) = (-1)^{(\frac{m-1}{2})(\frac{n-1}{2})}$$

这些性质的证明都留作练习，只简单说说(3)。设$n = p_1^{l_1} \cdots p_r^{l_r}$，则(3)归结为证明

$$\frac{p_1^{l_1} \cdots p_r^{l_r} - 1}{2} \equiv l_1 \frac{p_1 - 1}{2} + \cdots + l_r \frac{p_r - 1}{2} \pmod 2$$

归结为证明对任意奇数a, b有

$$\frac{a-1}{2} + \frac{b-1}{2} \equiv \frac{ab-1}{2} \pmod 2$$

这是很容易证明的。

用Jacobi符号，计算勒让德符号会更方便。因为算$(\frac{a}{p})$时不必分解a，例如

$(\frac{143}{353}) = (\frac{353}{143}) = (\frac{67}{143}) = -(\frac{143}{67}) = -(\frac{9}{67}) = -1$

$(\frac{129}{353}) = (\frac{353}{129}) = (\frac{95}{129}) = (\frac{129}{95}) = (\frac{34}{95}) = (\frac{2}{95})(\frac{17}{95}) = (\frac{17}{95}) = (\frac{95}{17}) = (\frac{10}{17}) = (\frac{5}{17}) = (\frac{17}{5}) = (\frac{2}{5}) = -1$

练习

1、（利用Jacobi符号）证明$2^n - 1 \dagger 3^n - 1$。你能否出一个类似的题。

2、设D为无平方因子的整数，用D^*表示

$$D^* = \begin{cases} D, \text{若} D \equiv 1 \pmod 4 \\ 4D, \text{其它} \end{cases}$$

证明对奇素数p, q，有

$$p \equiv q \pmod{D^*} \Longrightarrow (\frac{D}{p}) = (\frac{D}{q})$$

3、书中第121页第4、6、7、15、16、13(1)(2)；第155页第1、2

31 特殊的二次同余方程的解法

用二次互反律很容易判别二次同余方程

$$x^2 \equiv n \pmod{p} \tag{1}$$

是否有解，但如何解却不容易，在某些特殊情形下，解有某种表达式。

定理31.1. 设p为奇素数，$(\frac{n}{p})=1$，则
1) 当$p \equiv 3 \pmod 4$时，方程(1)的解为

$$x \equiv \pm n^{\frac{p+1}{4}} \pmod{p}$$

2)当$p \equiv 5 \pmod 8$时，方程(1)的解为

$$x \equiv \begin{cases} \pm n^{\frac{p+3}{8}} \pmod{p}, 若 n^{\frac{p-1}{4}} \equiv 1 \pmod{p} \\ \pm n^{\frac{p+3}{8}}(\frac{p-1}{2})! \pmod{p}, 若 n^{\frac{p-1}{4}} \equiv -1 \pmod{p} \end{cases}$$

证明：1) 因$n^{\frac{p-1}{2}} \equiv 1 \pmod p$，但$\frac{p-1}{2}$是奇数（加1后变成偶数），故

$$n \equiv n^{\frac{p-1}{2}+1} = (n^{\frac{p+1}{4}})^2 \pmod{p}$$

得出(1)的解。
2) 仍然$n^{\frac{p-1}{2}} \equiv 1 \pmod p$，但$\frac{p-1}{2}$是偶数，不过只有一个2因子，此时

$$n^{\frac{p-1}{4}} \equiv \pm 1 \pmod{p}$$

分两种情形：若$n^{\frac{p-1}{4}} \equiv 1 \pmod p$，因$\frac{p-1}{4}$已经是奇数，故由1)的方法可得解为

$$x \equiv \pm n^{\frac{p+3}{8}} \pmod{p}$$

若$n^{\frac{p-1}{4}} \equiv -1 \pmod p$，则

$$n \equiv -(n^{\frac{p+3}{8}})^2 \equiv (p-1)!(n^{\frac{p+3}{8}})^2 \equiv (\frac{p-1}{2}!)^2(n^{\frac{p+3}{8}})^2 \pmod{p}$$

从而得出方程(1)的解。

注：情形1)指ord $_2(p-1)=1$；情形2)指ord $_2(p-1)=2$，如果借助一个给定的非二次剩余c，解可以表示得简单一些，因$c^{\frac{p-1}{4}}$可代替$\frac{p-1}{2}!$，这样的方法可自然推广到ord $_2(p-1) \geq 3$（即$p \equiv 1 \pmod 8$）的情形，只是复杂些，见数论讲义110页定理2，留作练习。

定理31.2. 设p为奇素数，$(\frac{n}{p})=1$，则对任意正整数l
方程

$$x^2 \equiv n \pmod{p^l} \tag{2}$$

有两个解

证明：记$f(x)=x^2-n$，设(1)的解为$\pm x_0$，则$f'(\pm x_0) = \pm 2x_0 \not\equiv 0 \pmod p$，因此由Hensel引理得到所要结论。

注：当$p=2$时，方程(2)何时有解会更困难，作为练习讨论在什么条件下方程(2)有解。

32 素数表平方和

定理32.1. 设p为素数，则p可表为平方和当且仅当$p=2$或$p\equiv 1 \pmod 4$

必要性是显然的。由于$p\equiv 1 \pmod 4 \Longrightarrow$ 存在整数m,有$p|m^2+1$。因此上述定理可由下列定理推出

定理32.2. m^2+1形的数的素因子都是平方和。

这个定理的证明需要一个引理

引理32.3. 若$(x,y)=1$，称x^2+y^2为本原平方和。如果一个本原平方和x^2+y^2的素因子p可表为平方和，则$\frac{x^2+y^2}{p}$也可表为本原平方和。

证明：设$p=a^2+b^2$，则

$$a^2\equiv -b^2 \pmod p$$

$$x^2\equiv -y^2 \pmod p$$

于是

$$a^2x^2\equiv b^2y^2 \pmod p$$

$$ax\equiv \pm by \pmod p$$

若$ax\equiv by \pmod p$（另一种情形同样证明，省略），则

$$\frac{x^2+y^2}{p}=\frac{(a^2+b^2)(x^2+y^2)}{p^2}=\frac{(ax-by)^2+(ay+bx)^2}{p^2}=(\frac{ax-by}{p})^2+(\frac{ay+bx}{p})^2$$

但由$p|ax-by$和$p|(a^2+b^2)(x^2+y^2)=(ax-by)^2+(ay+bx)^2$知$p|ay+bx$，因此$\frac{x^2+y^2}{p}$表为平方和

$$(\frac{ax-by}{p})^2+(\frac{ay+bx}{p})^2$$

现证明这种表示是本原的，若有$d|(\frac{ax-by}{p},\frac{ay+bx}{p})$，则

$$d|a\frac{ax-by}{p}+b\frac{ay+bx}{p}=x$$

同理$d|y$。由于$(x,y)=1$，故$d=1$。表示是本原的。

现在证明定理4.10.2：对m作归纳。$m=1$时显然成立。假设对$<m$的整数成立。任取素数$p|m^2+1$，若$p<m$，则由$p|(m-p)^2+1$和归纳假设知p是平方和。若$p>m$，则$\frac{m^2+1}{p}=p_1\cdots p_r<m$，当然每个$p_i<m$，于是$p_i$是平方和，再由引理可得$p=\frac{m^2+1}{p_1\cdots p_r}$是（本原）平方和。

定理4.10.1也随之得证。

33 Gauss整数的算术

注意到$a^2+b^2=(a+bi)(a-bi)$，前面的证明都可以在Gauss整数$\mathbb{Z}[i]=\{a+bi|a,b\in\mathbb{Z}\}$中进行。我们说$\mathbb{Z}[i]$按照加法和乘法构成环，称为Gauss整数环。我们先把$\mathbb{Z}$上的算术理论搬到Gauss整数环上。

命题33.1. $\mathbb{Z}[i]$上的单位（即可以求倒数的元）只有$\pm 1,\pm i$

证明:设$a+bi$是$\mathbb{Z}[i]$上的单位，则$\frac{1}{a+bi}=\frac{a-bi}{a^2+b^2}\in\mathbb{Z}[i]$，即$\frac{a}{a^2+b^2},\frac{b}{a^2+b^2}\in\mathbb{Z}$。从而$a+bi=\pm 1,\pm i$

定义33.2. 称α为$\mathbb{Z}[i]$上的“素元”，如果α的每一个因子β，都有β或$\frac{\alpha}{\beta}$是单位。

定理33.3. 对复数$\alpha = a + bi$，用$N(\alpha)$表$a^2 + b^2$。对任意$\alpha, \beta \in \mathbb{Z}[i]$，$\beta \neq 0$，存在$\gamma, \lambda \in \mathbb{Z}[i]$，满足

$$\alpha = \lambda\beta + \gamma 和 N(\gamma) < N(\beta)$$

；也可以换种说法存在$\gamma \in \mathbb{Z}[i]$满足

$$\alpha \equiv \gamma \pmod{\beta} 和 N(\gamma) < N(\beta)$$

证法一（几何法）：不妨设$N(\alpha) \geq N(\beta)$，而且α与β（作为向量）不共线，断言:存在$u = \pm 1, \pm i$，使$|\alpha - u\beta| < |\alpha|$（这样重复进行即可完成证明）。首先可取$u_1 = \pm 1$，使$\alpha$与$u_1\beta$夹角为锐角；然后可取$u_2 = \pm i$，使$\alpha$与$u_2u_1\beta$夹角不超过45度。简单从三角形可看出$|\alpha - u_2u_1\beta| < |\alpha|$ 证法二：$\frac{\alpha}{\beta} = \lambda + \delta$，这里

$$\lambda \in \mathbb{Z}[i], \delta = a + bi, a, b \in \mathbb{Q}, |a| \leq \frac{1}{2}, |b| \leq \frac{1}{2}$$

于是$N(\delta) = a^2 + b^2 \leq \frac{1}{2} < 1$。并且

$$\alpha = \lambda\beta + \delta\beta$$

一方面

$$\delta\beta = \alpha - \lambda\beta \in \mathbb{Z}[i]$$

另一方面

$$N(\delta\beta) = N(\delta)N(\beta) < N(\beta)$$

因此取$\gamma = \delta\beta$即完成证明

推论33.4. 对$\alpha, \beta \in \mathbb{Z}[i]$，集合$\alpha\mathbb{Z}[i] + \beta\mathbb{Z}[i]$一定形如$\gamma\mathbb{Z}[i]$

证明略，这样的γ称为α和β的最大公因子，它是集合$\alpha\mathbb{Z}[i] + \beta\mathbb{Z}[i]$中$N(\gamma)$最小的（即复绝对值最小）。

推论33.5. （$\mathbb{Z}[i]$上的唯一分解定理）$\mathbb{Z}[i]$上的任何非零元可唯一分解为“素元”之积

注：证明就是平推旧的证明（因为有带余除法），但请仔细体会唯一的含义。

定义33.6. $a + bi \in \mathbb{Z}[i]$称为本原的，若a与b互素

任何一个Gauss整数可写为一个普通整数乘一个本原的Gauss整数，因此需问什么普通素数还是“素的”，一个本原的Gauss整数何时是“素的”。

命题33.7. 普通素数p是“素的”当且仅当p不是平方和

证明：必要性是显然的，因为若$p = a^2 + b^2$，则$p = (a + bi)(a - bi)$。现证从分性：若p不是“素的”，则$p = (a + bi)(c + di)$，因而$p^2 = (a^2 + b^2)(c^2 + d^2), a^2 + b^2 > 1, c^2 + d^2 > 1$，说明$a^2 + b^2 = p = c^2 + d^2$，矛盾。

命题33.8. 本原的$Gauss$整数$a + bi$是“素的”当且仅当$a^2 + b^2$是素数

证明:先证从分性。若$a + bi$不是“素的”，那么$a + bi = (c + di)(A + Bi)$，且$a + bi, c + di$都非单位，于是$a^2 + b^2 = (c^2 + d^2)(A^2 + B^2)$ 非素数。再证必要性。若$a^2 + b^2$不是素数，则$a^2 + b^2 = mn$，m, n都是¿1的整数，但

$$(a + bi)(a - bi) = mn$$

且$a - bi$也必是“素的”，由于唯一分解性成立，必然m, n都是素数，且“素”，还必须m, n分别与$a + bi, a - bi$相伴（即差一个单位），但这是不可能的。

34 Gauss整数的应用

现在我们用Gauss整数的算术理论重新证明和解释关于平方和的定理。

先证定理4.10.2：若$p|m^2+1=(m+i)(m-i)$，显然$p\nmid m+i, p\nmid m+i$。由Gauss整数的唯一分解性知p不是“素的”。再由命题4.11.7知p是平方和。

虽然不需要引理4.10.3了，我们还是回头重证引理4.10.3了：

因为a^2+b^2=素数p，故由命题4.11.8知$a+bi$是“素的”，由条件$(a+bi)(a-bi)=p|x^2+y^2$知

$$a+bi|(x+yi)(x-yi)$$

必然$a+bi|x+yi$或$a+bi|x-yi$。若前者成立，记

$$(a+bi)(c+di)=x+yi$$

则有$(a^2+b^2)(c^2+d^2)=x^2+y^2$，即$c^2+d^2=\frac{x^2+y^2}{p}$。如果我们想知道$c,d$是多少，就：

$$c+di=\frac{x+yi}{a+bi}=\frac{(a-bi)(x+yi)}{a^2+b^2}=\frac{ax+by}{p}+\frac{ay-bx}{p}i$$

从而$c=\frac{ax+by}{p}, d=\frac{ay-bx}{p}$

我们再讲一个Gauss整数在不定方程中的应用。

例1 在整数范围内解方程$y^2+1=x^3$。

解：经过简单讨论知y为偶数。将方程变形为

$$(y+i)(y-i)=x^3$$

设法说明$y+i$与$y-i$“互素”。若它们有公共“素因子”π，则$\pi|2i=(1+i)^2$，即$\pi=1+i$，但因$y=2n=-i(1+i)^2n$，故$y+i\equiv i \pmod{1+i}$，说明$1+i\nmid y+i$。综上，$y+i$与$y-i$“互素”。由唯一分解定理知

$$y+i=u(a+bi)^3, u\text{是一单位}$$

由于所有单位$\pm1,\pm i$都是某元的三次方，故可设

$$y+i=(a+bi)^3$$

比较虚部知$1=3a^2b-b^3=b(3a^2-b^2)$。说明$b=\pm1$，进一步讨论知必须

$$b=-1, a=0$$

原方程解为

$$x=1, y=0$$

例2 在整数范围内解方程$x^2+y^2=z^{10}, (x,y)=1$。

解：简单讨论知x,y一奇一偶，易知$x+yi, x-yi$“互素”，因此$x+yi=u(a+bi)^10$，$u=\pm1,\pm i$给出全部解。

Gauss整数的研究显然给了我们（相比平方和问题本身）更多。特别是给我们以启发：即使我们只关心$\mathbb{Z}$中的问题，我们也常常需要跳到$\mathbb{Z}$以外去。关于Gauss整数环中的“素元”可以重新刻划如下：

(1)pu，p是一个$4k+3$形的素数，u是单位。

(2)满足$N(\alpha)$是普通素数的α

Gauss整数的算术理论还可推广到其他一些环$\mathbb{Z}[\sqrt{d}]$中，请想想，什么d使得$\mathbb{Z}[\sqrt{d}]$有好性质。

练习

1. 证明对任意Gauss整数$x+yi$，有

$$x+yi \equiv \begin{cases} 0 \pmod{1+i}, \text{若} x \equiv y \pmod 2 \\ 1 \pmod{1+i}, \text{若} x \not\equiv y \pmod 2 \end{cases}$$

2. 证明所有的素数中只有2有一特殊性质：在Gauss整数中有平方因子。
3. 研究$\mathbb{Z}[\sqrt{-2}]$的带余除法及唯一分解性，然后证明对奇素数p，

$$p\text{可表为}a^2+2b^2 \Longleftrightarrow (\frac{-2}{p})=1 \Longleftrightarrow p \equiv 1,3 \pmod 8$$

4. 解不定方程$y^2+2=x^3$
5.（思考题）解不定方程$y^2+5=x^3$

35 不定方程简介

如果要证明某方程$f(x_1,...,x_n)=0$无整数解，一个常见的想法是找一个适当的m使

$$f(x_1,...,x_n) \equiv 0 \pmod m$$

无解。
例1 求方程$x^2+y^2=3z^2$的非零整数解。
解法一：假设有解，不妨设x,y,z两两互素。取$p=3$，将原方程模3得

$$x^2 \equiv -y^2 \pmod 3,$$

从而得到-1是模3的二次剩余，不可能。
解法二：取$p=2$，将原方程模2^2得

$$x^2+y^2+z^2 \equiv 0 \pmod 4,$$

不可能。

注：原方程中将3换成任一模4余3的素数都一样。

例2 解方程

$$x^3+y^3+z^3=9u \pm 4$$

解：将原方程模9得

$$x^3+y^3+z^3 \equiv \pm 4 \pmod 9$$

由于$x^3 \equiv 0, \pm 1 \pmod 9$，故上式无解，原方程无解。

例3 解方程

$$y^2=x^3+(4b-1)^3-4a^2$$

其中a,b是给定整数，a无$4t+3$形的素因子。

解：首先x必须是奇的（否则x偶，y奇，对原方程两边模4即得到矛盾）。$x^3+(4b-1)^3=(x+4b-1)(x^2-(4b-1)x+(4b-1)^2)$，由于$0<x^2-(4b-1)x+(4b-1)^2)\equiv 3 \pmod 4$，因此存在$x^2-(4b-1)x+(4b-1)^2)$的素因子$p\equiv 3 \pmod 4$。对原方程模$p$得

$$y^2\equiv -4a^2,$$

但由条件知$a\not\equiv 0 \pmod p$，综合得到$(\frac{-1}{p})=-1$。得到矛盾。

下面讲述不定方程的柯召方法，它是柯先生在研究Catalan猜想时首创的。Catalan在1842年提出一个猜想：8和9是仅有的两个连续正整数，它们都是整数方幂。用不定方程的语言来说就是:当$m,n>1$时，方程

$$x^m+1=y^n$$

除了$m=3,n=2,x=2,y=3$以外没有其他的正整数解。

先简单分析一下：首先将一般问题归结为看似特殊的方程

$$x^p+1=y^q$$

p,q是不同的素数。再按p,q分成两类：

(1) p,q之一为2

(2) p,q都是奇。

(1)的一种情形$p=2$由Lebesque很快解决（只需在Gauss整环上进行即可），剩下一种是$q=2$，即下述柯召方程

$$x^p+1=y^2 \tag{1}$$

而其中$p=3$的情形则在猜想提出之前就已解决，剩下情形由柯召先生在1962年解决。方法是完全初等的，称为柯召方法，用它可以解决一大类不定方程。在柯先生的工作之前，数学大师Selberg（菲尔兹和沃尔夫双奖获得者）曾证明了较弱的情形，即方程

$$x^p+1=y^4$$

无解。在几年前，Catalan猜想的最后情形也解决了。

定理35.1. *柯召方程1)没有满足$(x+1,\frac{x^p+1}{x+1})>1$的正整数解*

注：$(x+1,\frac{x^p+1}{x+1})=1$的情形用其他方法证（先于我们这种情形解决），我们这种情形代表了柯召方法的精华。

证明：因为$(x+1,\frac{x^p+1}{x+1})=1$或$p$，故$(x+1,\frac{x^p+1}{x+1})=p$。但

$$y^2=(x+1)\frac{x^p+1}{x+1}$$

故有

$$x+1=py_1^2 \tag{2}$$

$$\frac{x^p+1}{x+1}=py_2^2 \tag{3}$$

由1)知x为偶数（否则y为偶数，从而$(y+1,y-1)=1$，进而$y\pm 1$都是p次幂，很容易得矛盾），再结合2)知

$$x+1\equiv p \pmod 8 \tag{4}$$

以下对p分情形讨论

(1)当$p \equiv 3,5,7 \pmod 8$时

我们在原方程1)上造矛盾，取适当的模对两边算jacobi符号，右边是1，如果左边是-1即可。

先取模$x-1$。因$x^p+1 \equiv 2 \pmod{x-1}$，故

$$(\frac{x^p+1}{x-1}) = (\frac{2}{x-1}) = (\frac{2}{p-2})$$

（由此可知$p \equiv 5,7 \pmod 8$时已解决）

再取模x^3-1。因$x^p+1 \equiv x+1$或$x^2+1 \pmod{x^3-1}$，故分别计算

$$(\frac{x+1}{x^3-1}) = (-1)^{\frac{x+1-1}{2}}(\frac{x^3-1}{x+1}) = (\frac{-1}{x+1})(\frac{-2}{x+1}) = (\frac{2}{x+1}) = (\frac{2}{p})$$

$$(\frac{x^2+1}{x^3-1}) = (\frac{x^3-1}{x^2+1}) = (\frac{-x-1}{x^2+1}) = (\frac{x+1}{x^2+1}) = (\frac{x^2+1}{x+1}) = (\frac{2}{x+1}) = (\frac{2}{p})$$

即

$$(\frac{x^p+1}{x^3-1}) = (\frac{2}{p})$$

综上，当$p \equiv 3,5,7$时，总有

$$(\frac{x^p+1}{x-1}) = -1 \text{或} (\frac{x^p+1}{x^3-1}) = -1$$

得到矛盾。

(2)当$p \equiv 1 \pmod 8$时，对方程3)造矛盾。记

$$E(a) = \frac{(-x)^a-1}{-x-1},$$

当然在a为奇时$E(a) = \frac{x^a+1}{x+1}$。现取模$E(a)$计算Jacobi符号。柯先生发现对$a<p$，总有

$$(\frac{E(p)}{E(a)}) = 1$$

但取适当的a，可使

$$(\frac{py_2^2}{E(a)}) = -1$$

从而得到矛盾。

观察：因为对任意正整数m,n,t，只要$m \equiv n \pmod t$，就有

$$(-x)^m - 1 \equiv (-x)^n - 1 \pmod{(-x)^t-1}$$

从而

$$E(m) \equiv E(n) \pmod{E(t)}$$

$$(E(m), E(n)) = E((m,n))$$

当$(m,n)=1$时，有

$$(E(m), E(n)) = E(1) = 1$$

对$0<a<p$，有$(a,p)=1$，故可做辗转相除法

$$p \equiv a_1 \pmod a$$

$$a \equiv a_2 \pmod{a_2}$$

$$\cdots$$

$$a_{n-2} \equiv a_n = 1 \pmod{a_{n-1}}$$

相应地

$$E(p) \equiv E(a_1) \pmod{E(a)}$$

$$E(a) \equiv E(a_2) \pmod{E(a_1)}$$

$$\cdots$$

$$E(a_{n-2}) \equiv E(a_n) = 1 \pmod{E(a_{n-1})}$$

另外，由4)知$x \equiv 1 \pmod 8$，故$E(p), E(a), E(a_i) \equiv 1 \pmod 8$，于是有以下计算

$$(\frac{E(p)}{E(a)}) = (\frac{E(a_1)}{E(a)}) = (\frac{E(a)}{E(a_1)}) = (\frac{E(a_2)}{E(a_1)}) = \cdots = (\frac{E(1)}{E(a_{n-1})}) = 1$$

但

$$(\frac{py_2^2}{E(a)}) = (\frac{p}{E(a)}) = (\frac{E(a)}{p}) = (\frac{a}{p})$$

最后一个等式是因为$-x \equiv 1 \pmod p$（见方程2)）。因此只要取奇数a使$(\frac{a}{p}) = -1$即可得到需要的矛盾。

数论函数

第十一周 基本数论函数与解析方法

36 几个常见数论函数

称自变量取正整数的函数为数论函数，不过我们关心的是有数论背景的函数。我们将会看到所有数论函数形成一个交换环。有时，我们也把取整函数$[\cdot]$称为数论函数。现在分别讨论几种常见函数：

•取整函数$[\cdot]$只需注意以下性质

(1) $[x+y] \geq [x] + [y]$

(2) 对整数n，有$[x+n] = [x] + n$

(3) $[\frac{[\frac{x}{a}]}{b}] = [\frac{x}{ab}]$

证明全都留作练习。

•函数$\mathrm{pot}_p \cdot$(或记为$\mathrm{ord}_p \cdot$)

对任意正整数a，和素数p，若$p^r || a$，称p^r为a的p部分，记$r = \mathrm{pot}_p a$，显然有以下性质：

(1) $\mathrm{pot}_p ab = \mathrm{pot}_p a + \mathrm{pot}_p b$

(2) $\mathrm{pot}_p (a+b) \geq \min(\mathrm{pot}_p a, \mathrm{pot}_p b)$

上式在$\mathrm{pot}_p a \neq \mathrm{pot}_p b$时一定取等号。

也可按如下方式将pot_p扩充定义域到非零有理数集$\mathbb{Q}^*$：

$\mathrm{pot}_p(-a) = \mathrm{pot}_p a$，$\mathrm{pot}_p \frac{n}{m} = \mathrm{pot}_p n - \mathrm{pot}_p m$，

或等价地定义为当$a = p^r \cdot \frac{n}{m}$，$r, m, n \in \mathbb{Z}, (p, m) = (p, n) = 1$时，

$$\mathrm{pot}_p a = r$$

显然，上述两条性质仍然成立，举例说明它的应用:

若$a = 1 + \frac{1}{2} + \cdots + \frac{1}{20}$，故反复用性质(2)可知对$p = 11, 13, 17, 19$

$$\mathrm{pot}_p a = -1$$

这不仅说明a非整数，进一步a的分母m满足

$$\mathrm{pot}_p m = 1;$$

再取$p=2$，$\mathrm{pot}_2 \frac{1}{16} = -4$；对$1,2,...,20$中任何$n \neq 16$，有$\mathrm{pot}_2 \frac{1}{n} \geq -3$。因此反复用性质(2)知

$$\mathrm{pot}_2 a = -4$$

进一步可对$p=3,5,7$用类似方法计算$\mathrm{pot}_p a$，从而完全确定a的分母

$$2^4 \times 3 \times 7 \times 11 \times 13 \times 17 \times 19$$

定理36.1. 对任意素数p和正整数n，有

$$pot_p n! = [\frac{n}{p}] + [\frac{n}{p^2}] + \cdots$$

证明：设$m = [\frac{n}{p}]$，则因

$$n! = 1 \cdots p \cdots 2p \cdots mp \cdot (mp+1) \cdots n$$

可知

$$\mathrm{pot}_p n! = \mathrm{pot}_p (p^m m!) = m + \mathrm{pot}_p m! \qquad *$$

归纳并注意到$[\frac{n}{ij}] = [\frac{[\frac{n}{i}]}{j}]$可得定理需要的公式。

定理36.2. 对任意素数p和正整数n，记$A(n,p)$为n的p进展开式的各位数字之和，则有下列公式

$$pot_p n! = \frac{n - A(n,p)}{p-1}$$

证明：还是利用$*$式进行归纳，因此只需检查

$$m + \frac{m - A(m,p)}{p-1} = \frac{n - A(n,p)}{p-1} ?$$

对p做带余除法$n = pm + a_0$，那么$A(n,p) = a_0 + A(m,p)$，简单计算可知上式成立。

- 因子函数$d(n) := n$的因子个数。
- 因子和函数$\sigma(n) := \sum_{d|n} d$
- $I(n) = \begin{cases} 1, n=1 \\ 0, n>1 \end{cases}$
- $e(n) = 1$
- Mobius函数μ：

$$\mu(n) = \begin{cases} 1, n=1 \\ 0, n\text{有平方因子} \\ (-1)^r, n\text{是}r\text{个不同素数之积} \end{cases}$$

定理36.3.

$$\sum_{d|n} \mu(d) = \begin{cases} 1, n=1 \\ 0, n>1 \end{cases}$$

证明：对$n>1$，设$n=p_1^{l_1}\cdots p_r^{l_r}$，则

$$\sum_{d|n}\mu(d)=\sum_{d|p_1\cdots p_r}\mu(d)=\sum_{i=0}^{r}(-1)^i\binom{p}{i}=0$$

• Euler函数ϕ：

我们已经学过了Euler函数$\phi(n)$，这里只简单重复一下基本性质:

(1) 乘性：对$(m,n)=1$，有

$$\phi(mn)=\phi(m)\phi(n)$$

(2) $\sum_{d|n}\phi(d)=n$

上式可简单解释为对n阶循环群中的元按（元素的）阶分类计数。

(3) 用$\mu(n)$的语言重新表述

$$\phi(n)=\sum_{d|n}\mu(d)\frac{n}{d}$$

37 数论函数的运算和相互关系

对数论函数$f(n)$和$g(n)$，定义函数

$$(f*g)(n)=\sum_{d|n}f(d)g(\frac{n}{d})=\sum_{d_1d_2=n}f(d)g(\frac{n}{d})$$

为$f(n)$和$g(n)$的Dirichlet乘积。显然乘积是交换的，事实上也有结合律，即

$$(f(n)*g(n))*h(n)=f(n)*(g(n)*h(n))$$

证明是简单计算，两端都等于

$$\sum_{abc=n}f(a)g(b)h(c)$$

当然也可按通常方式定义加法，这样所有数论函数形成一个交换环。乘法单位元是$I(n)$

对数论函数$f(n)$，可定义一个新的数论函数$g(n)=\sum_{d|n}f(d)$为它的Mobius变换。Euler函数的性质(2)是说ϕ的Mobius变换是恒等函数$h(n)=n$，性质(3)意味着ϕ可由h得到，一般地有下列Mobius反演公式：

$g(n)=\sum_{d|n}f(d)\Rightarrow f(n)=\sum_{d|n}g(d)\mu(\frac{n}{d})$

因而，称$f(n)=\sum_{d|n}g(d)\mu(\frac{n}{d})$为Mobius逆变换。反演公式的证明可通过直接计算（练习）或下列方式得到；

将f的Mobius变换改写为$f*e$，再将g的Mobius逆变换改写为$g*\mu$。因此Mobius反演公式归结为

$$e*\mu=I$$

但这正是μ的基本性质。

另外Mobius反演公式还有如下乘积形式:

$$g(n)=\prod_{d|n}f(d)\Longrightarrow f(n)=\prod_{d|n}g(d)^{\mu(\frac{n}{d})}$$

f的值域可以不是数集合而是某个乘法交换群，或某个域。例如：记ζ_n为n次本原单位根，即复数乘法群中的一个n阶元。那么全体n次单位根为$\zeta_n^j,j=1,2,...,n$;全体n次本原单位根为ζ_n^j，$(j,n)=1$。记

$$\phi_n(x)=\prod_{j=1,(j,n)=1}^{n}(x-\zeta_n^j)$$

那么

$$x^n - 1 = \prod_{d|n} \phi_d(x)$$

由乘法形式的Mobius反演公式得

$$\phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(\frac{n}{d})}$$

注：Dirichlet乘积的背景是Dirichlet对数论函数$f(n)$引进一个级数

$$L_f(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}$$

这样的级数可以形式地定义乘法，并且有

$$L_{f*g}(s) = L_f(s) L_g(s)$$

由于级数（只要f不太坏）在s充分大时可表示一个具有好性质的函数（解析函数），于是可望通过分析方法研究数论（函数）。

练习

1、证明前面未证明的结论。

2、思考Mobius反演公式与容斥原理的关系，能否有一个统一的定理。

38 素数分布

由于时间关系，我们没法走得更远，只能以讲座形式简介数论的两类基本问题之一的素数分布。

定义38.1. $\pi(n)$表示不超过n的素数的个数。

关于$\pi(n)$，我们有如下认识:

(1) $\pi(n) \longrightarrow \infty$

这就是说素数有无限多，Eucilid就已经证明了，现在我们用Euler的分析方法证一遍。记

$$\zeta(s) = \sum_{i=1}^{\infty} \frac{1}{n^s}$$

它是常函数$I(n)$的Diricheli级数，现在把它当成关于s的实函数，当$s > 1$时，级数收敛，且（由算术基本定理知）

$$\zeta(s) = \prod_p (1 + p^{-s} + p^{-2s} + \cdots) = \prod_p (1 - p^{-s})^{-1}$$

$$\log \zeta(s) = \sum_p (-\log(1 - p^{-s})) = \sum_p \sum_{m=1}^{\infty} \frac{p^{-ms}}{m} = \sum_p p^{-s} + \sum_p \sum_{m=2}^{\infty} \frac{p^{-ms}}{m} \tag{1}$$

对$\sum\limits_p \sum\limits_{m=2}^{\infty} \frac{p^{-ms}}{m}$做简单估计：

$$0 < \sum_p \sum_{m=2}^{\infty} \frac{p^{-ms}}{m} < \sum_p \sum_{m=2}^{\infty} p^{-m} = \sum_p \frac{p^{-2}}{1 - p^{-1}} = \sum_p \frac{1}{p(p-1)} < \sum_{n=2}^{\infty} \frac{1}{n(n-1)} = 1$$

当$s \longrightarrow 1^+$时(1)式左边是无穷，说明$\sum\limits_p p^{-s}$也是无穷，说明素数必须是无限多，且

$$\sum_p p^{-1} = \infty$$

(2) $\frac{\pi(n)}{n} \longrightarrow 0$
(3) $\frac{1}{8} \cdot \frac{n}{\log n} < \pi(n) < 6\frac{n}{\log n}$
(4) 素数定理

$$\pi(n) \sim \frac{n}{\log n}$$

(5) Riemann假设:对任意$\varepsilon > 0$，

$$\pi(n) - \frac{n}{\log n} = O(n^{\frac{1}{2}+\varepsilon})$$

即存在常熟C使$|\pi(n) - \frac{n}{\log n}| < Cn^{\frac{1}{2}+\varepsilon}$

显然(3) $\Longrightarrow$ (2)，但(3)不能导出(4)。(5)当然难于上青天。这些问题都与$\zeta(s) = \sum\limits_{i=1}^{\infty} \frac{1}{n^s}$ 有关。(3)称为切比雪夫定理，现证之：

首先通过对素数p的阶估计可得

$$\prod_{n<p\leq 2n} p | \frac{(2n)!}{n!n!} | \prod_{p\leq 2n} p^{r_{p,n}},$$

这里，$r_{p,n}$表满足$p^r \leq 2n$的最大r。因此有以下不等式

$$n^{\pi(2n)-\pi(n)} < \prod_{n<p\leq 2n} p \leq \binom{2n}{n} \leq \prod_{p\leq 2n} p^{r_{p,n}} \leq (2n)^{\pi(2n)}$$

经过粗约的估计有

$$2^n \leq \binom{2n}{n} < 2^{2n}$$

综上有

$$n^{\pi(2n)-\pi(n)} < 2^{2n}, 2^n < (2n)^{\pi(2n)}$$

取$n = 2^h$，有

$$h(\pi(2^{h+1}) - \pi(2^h)) < 2^{h+1} \tag{2}$$

$$2^h < (h+1)\pi(2^{h+1}) \tag{3}$$

我们将从(2)和(3)分别推出两个方向的所需不等式：

由(2)式得

$$(h+1)\pi(2^{h+1}) - h\pi(2^h) < 2^{h+1} + \pi(2^{h+1}) < \frac{3}{2}2^{h+1}$$

取$h = 0, 1, ..., k$并求和得

$$(k+1)\pi(2^{k+1}) < 3 \cdot 2^{k+1}$$

$$\pi(2^{k+1}) < 3 \cdot 2^{k+1}/(k+1)$$

对任意n，取k满足$2^k \leq n < 2^{k+1}$，于是

$$\pi(n) \leq \pi(2^{k+1}) < 3 \cdot 2^{k+1}/(k+1) < 3(2n)/\log_2 n < 6\frac{n}{\log n}$$

另一方面，由(3)式有

$$\pi(n) \geq \pi(2^k) > \frac{1}{2}\frac{2^k}{k} > \frac{1}{4}\frac{n}{\log_2 n} > \frac{1}{8}\frac{n}{\log n}$$

（最后一步用了$e < 4$）以上都是在数（某个界以内）所有素数，现在数一下对给定整数m，满足$x \equiv a \pmod m$的素数。当然在a与m不互素时，几乎没有素数。因此只需考查当$(a, m) = 1$时

定理38.2. 当$(a,m)=1$时，满足$x\equiv a\pmod m$的素数有无限个。

这是著名的Dirichlet定理，证明的思想是推广Euler证明素数无限的方法。我们来试着证$m=q$（素数），$a=1$的情形：

模仿Euler的做法，Dirichlet注意到对完全积性函数$\lambda(n)$，有以下类似公式

$$L(\lambda,s):=\sum_{i=1}^{\infty}\frac{\lambda(n)}{n^s}=\prod_p(1-\lambda(p)p^{-s})^{-1}$$

只要λ有界，可做类似分析得

$$\log L(\lambda,s)=\sum_p(-\log(1-\lambda(p)p^{-s}))=\sum_p\lambda(p)p^{-s}+\text{有界量}$$

如果λ满足

$$\lambda(n)=\begin{cases}1,n\equiv 1\pmod q\\0,\text{其它}\end{cases}\tag{4}$$

那么需证的结果归结为：左边是无穷（当s趋于1时）。

以上就是Dirichlet的基本思想，但一个函数λ难以兼顾两条好性质，而改用几个函数联手：

首先取定一个模q的原根g，对任意给定的$q-1$次复单位根ω，可定义一个从$(\mathbb{Z}/q\mathbb{Z})^\times$到$\mathbb{C}^\times$的乘法群同态$\chi_\omega$

$$\chi_\omega(g^m)=\omega^m$$

即

$$\chi_\omega(n)=\omega^{ind_g n}$$

补充定义$\chi_\omega(n)=0$将χ_ω的定义域扩充到$(\mathbb{Z}/q\mathbb{Z})$上，再通过与自然映射$\mathbb{Z}\longrightarrow\mathbb{Z}/q\mathbb{Z}$的合成将$\chi_\omega$看作定义在$\mathbb{Z}$上，从而得到完全积性的（复值）数论函数（仍记为$\chi_\omega$）。虽然$\chi_\omega$不满足(4)式的性质，但$\sum\limits_\omega\chi_\omega$却具有类似性质，即

$$\sum_\omega\chi_\omega(n)=\begin{cases}q-1,n\equiv 1\pmod q\\0,\text{其它}\end{cases}$$

于是有

$$\sum_\omega\log L(\chi_\omega,s)=\sum_p(\sum_\omega\chi_\omega(p))p^{-s}+\text{有界量}=\sum_{p\equiv 1\pmod q}(q-1)p^{-s}+\text{有界量}$$

最终需证明$\prod\limits_\omega L(\chi_\omega,s)$趋于无穷。易知$L(1,s)=(1-q^{-s})\zeta(s)$。下列关键的分析性质给出一切：当$\omega\neq 1$时，$L(\chi_\omega,1)\neq 0$。

以上函数作为复变函数（即s取复变量）最易看清本质。是Riemann首先把s当作复变量，通过前面的推导容易看出这些L函数的零点对数素数很重要。

39 复习举例

1. 证明对任意整数$n>1$，$2^n\not\equiv 1\pmod n$

证明：我们不把整个证明都写出来，只分几种情形说明想法。

(1) 若$n=p$，由Fermat小定理知$2^p\equiv 2\not\equiv 1\pmod p$；

(2) 若$n=p^2$，设$2^{p^2}\equiv 1\pmod{p^2}$，则$2^{p^2}\equiv 1\pmod p$，仍然Fermat小定理得到矛盾；

(3) 若$n=pq$，p,q均为素数，并且$2^n\equiv 1\pmod n$，于是$2^{pq}\equiv 1\pmod{pq}$，自然$2^{pq}\equiv 1\pmod p$。由于$pq\equiv q\pmod{p-1}$，因此由Fermat小定理知$2^q\equiv 1\pmod p$。由于q是素数，故2模p的阶就是q，因

此$q|p-1$;同理$q|p-1$，这两式必然互相矛盾。

2. 设有同余方程

$$x^8 \equiv 2 \pmod{73} \tag{1}$$

和

$$x^8 \equiv 1 \pmod{73} \tag{2}$$

依次回答以下问题，最终求解方程(1).
（1）方程(1)是否有解。
（2）求出方程(1)的一个解。
（3）求方程(1)和(2)的全体解。

解：（1）经计算$2^9 \equiv 1 \pmod{73}$，故方程(1)有解。
（2）由于$2^9 \equiv 1 \pmod{73}$，而$8 \times 8 \equiv 1 \pmod{9}$，故

$$2 \equiv 2^{8\times 8} \equiv (2^8)^8 \pmod{73}$$

即方程(1)的一个解是$2^8 \equiv 37 \pmod{73}$
（3）求方程(2)的解需求出一个模73的阶恰为8的元。为此先找一非二次剩余5（计算勒让德符号略），那么$5^{9\times 4} \equiv -1 \pmod{73}$，于是$5^9$应该是阶为8的元，经计算$5^9 \equiv 10 \pmod{73}$，即10是一8阶元，因此：
方程(2)的解为$x \equiv 10^k \pmod{73}, k = 0, 1, ..., 7$，
方程(1)的解为$x \equiv 37 \times 10^k \pmod{73}, k = 0, 1, ..., 7$

注：应当弄清每一步的道理，总结相应的知识点和数学思想。

3、设$m = 7^2 \times 13$，
（1）求2模m的阶
（2）找一个模m的阶最大的元。

解：（1）容易验证2模7的阶是3，于是2模7^2的阶是3或3×7（理由：$a^r \equiv 1 \pmod{p} \Rightarrow a^{pr} \equiv 1 \pmod{p^2}$），但显然有$2^3 \not\equiv 1 \pmod{7^2}$，故于是2模$7^2$的阶只能是$3 \times 7$；再求2模13的阶：$2^6 \equiv (\frac{2}{13}) \equiv -1 \pmod{13}$，$2^4 \not\equiv 1 \pmod{13}$，于是2模13的阶是12。因此求2模$m$的阶是$[21, 12] = 84$
（2）由于模m的最大阶是$[\phi(7^2), \phi(13)] = 84$，故2就是一个模$m$的阶最大的元。

练习

1、问模$7^2 \times 13$的阶最大的元有多少个？
2、证明若$n|a^n - b^n$，则$n|\frac{a^n-b^n}{a-b}$
3、若整数a模p^n的阶为r_n，则存在整数N，满足
当$n \le N$时，$r_n = r_N$；当$n > N$时$r_n = pr_{n-1}$。并对$a = 30$，$p = 5$考察相应的数列r_n，指出N。
4、设a是交换群G中一个元，p是素数，证明若a^{p^m}的阶是p^n，则a的阶是p^{m+n}
5、求1000以内使得$7n + 6$是立方数的正整数n的个数。
6、求满足$2^{100}|1999^m - 1$的最小正的m。
7、设m是与6互素的自然数。证明：$4^m - (2 + \sqrt{2})^m$的整数部分可被112整除。
8、证明对正整数n，$1^{1987} + 2^{1987} + \cdots + n^{1987}$不是$n + 2$的倍数。
9、证明：当$n > 1$时，不存在奇素数p和正整数m满足$p^n + 1 = 2^m$。
10、证明不定方程$x^2 + y^2 + z^2 = x^2y^2$无正整数解。

第十二周 群论总体设想

40 几个基本定理

第二同态基本定理

定理40.1. 第二同态基本定理
群版本：设有群的满同态$\phi: G \longrightarrow G'$，则

$$A \mapsto \phi(A), B \mapsto \phi^{-1}(B)$$

给出G的包含$Ker\phi$的子群和G'的子群之间的一对（互逆的）一一对应，并且正规子群对应正规子群。进一步，对一对对应的$A \triangleleft G$与$B \triangleleft G'$，我们有

$$G/A \cong G'/B$$

环版本: 设有环的满同态$\phi: R \longrightarrow R'$，则

$$I \mapsto \phi(I), J \mapsto \phi^{-1}(J)$$

给出R的包含$Ker\phi$的理想和B的理想之间的一对（互逆的）一一对应。进一步，我们有

$$A/I \cong B/J$$

证明：我们只证群版本，环版本完全一样证。由于ϕ是满的，故简单的集合论告诉我们

$$\phi(\phi^{-1}(B)) = B$$

我们只需证

$$\phi^{-1}(\phi(A)) = A \tag{1}$$

第一同态度基本定理的本质是$\phi^{-1}(\phi(a)) = a\mathrm{Ker}\phi$，因此，对$A < G$，有

$$\phi^{-1}(\phi(A)) = \cup_{a\in A}\phi^{-1}(\phi(a)) = \cup_{a\in A}a\mathrm{Ker}\phi = A\mathrm{Ker}\phi$$

此外若$A \supset \mathrm{Ker}\phi$，则因$A\mathrm{Ker} = A$，保证了(1)式。

此外当B正规时，对合成映射

$$G \longrightarrow G' \longrightarrow G'/B$$

用同态基本定理可知$A = \phi^{-1}(B)$（正好是核）也正规，且有同构关系；若已知A正规，则对任意$y = \phi(x) \in G'$，有

$$yBy^{-1} = \phi(x)\phi(A)\phi(x^{-1}) = \phi(xAx^{-1}) = \phi(A) = B$$

即B正规。

上一个定理中，只考察了G的包含$\mathrm{Ker}\phi$的子群，而人为地无视其它子群，现在考察任意$A < G$，记ϕ_A为ϕ在A中的限制，对满同态$\phi_A : A \longrightarrow \phi(A)$用同态基本定理有$G/\mathrm{Ker}\phi_A \cong \phi(A)$，而$\mathrm{Ker}\phi_A = \mathrm{Ker}\phi \cap A$，故得下列定理：

定理40.2. 设有群的满同态$\phi: G \longrightarrow G'$，则对$G$的任意子群$A$有

$$A/A \cap Ker\phi \cong \phi(A)$$

如果将$\phi: G \longrightarrow G'$换成$\pi: G \longrightarrow G/H$，上述两个定理可分别翻译为

定理40.3. 设G是群，H是G的正规子群，则G/H的每一个子群可唯一表为K/H，$H < K < G$。此外K/H正规当且仅当K正规，这时还有

$$G/K \cong (G/H)/(K/H)$$

定理40.4. 设G是群，H是G的正规子群，$K < G$，则

$$K/K \cap H \cong KH/H$$

41 本章概论

研究群这样的抽象结构，首要的是分类问题。首先有如下初级的分类：
有限群和无限群；abel群和非abel群；有限生成的群和非有限生成的群。

以上的分法都太粗了，最好是能完全按同构分类，即给一张无限大（但可以描述）的表，表上每个位置放一个群，不同位置的群不同构，任意的群都同构于表上的某一个群。但这样的分类几乎是不可能实现的。但我们将看到对有限生成abel群完成了这样的分类。

对群G的研究，原则上可通过取一个正规子群$H \lhd G$简化为对两个较简单的群H和G/H的研究，这样的理论称为群的扩张理论（本课程不会细讲）。称G是两个群K_1和K_2的扩张如果存在正规子群$H \lhd G$使得H和商群G/H分别同构于K_1和K_2.
例：我们知道6阶群有两个，即$\mathbb{Z}/6\mathbb{Z}$和S_3，他们都有3阶正规子群

$$2\mathbb{Z}/6\mathbb{Z} \lhd \mathbb{Z}/6\mathbb{Z}, \quad A_3 \lhd S_3$$

当然商群是2阶。换句话说两个6阶群就是$\mathbb{Z}/3\mathbb{Z}$和$\mathbb{Z}/2\mathbb{Z}$的（全部）扩张。

进一步，只要对H和G/H继续用上面方法化简，我们得到可以通过一个次正规列

$$1 = G_n \lhd G_{n-1} \lhd \cdots \lhd G_1 \lhd G_0 = G$$

G是这些商群$G_i/G_{i+1}, i = 0, ..., n-1$做多次扩张得到（这里反复使用了第二同态定理），于是有下列概念：

- **可解群** 群G称为可解群，如果存在一个次正规列

$$1 = G_n \lhd G_{n-1} \lhd \cdots \lhd G_1 \lhd G_0 = G$$

使得每个商群$G_i/G_{i+1}, i = 0, ..., n-1$都是abel群。
- **单群** 群G称为单群，如果G没有非平凡的正规子群。

注：可解群即是那些可通过abel群做多次扩张得到的群，S_3是最小的可解的非abel群；单群就是不能由任何非平凡的群做扩张得到的群。

命题41.1. 有限交换的单群一定是素数阶

证明：若G的阶是和数n，任取非单位的元$a \in G$，a的阶是$m > 1$，取素数$p|m$，则$a^{\frac{m}{p}}$的阶是p，它生成一个p阶子群，必然是非平凡的（正规）子群，与G是单群矛盾。

现在给出可解群的另一常见刻画。

• **交换子** 群G的交换子是G的由所有$[a,b] := aba^{-1}b^{-1}, a,b \in G$生成的子群，记为$G^{(1)}$。它由下列性质刻画

1) $G^{(1)} \lhd G$

2) $G/G^{(1)}$**是abel的**

3) 任何满足$H \lhd G$, G/H**交换的**H，**必有**$G^{(1)} < H$

注: 3)可改为G到任何abel群的同态可通过$G/G^{(1)}$分解。因此有下列概念：

• **abel化** $G/G^{(1)}$称为G的abel化，记为G^{ab}。它是G的最大abel商。

显然G是abel的当且仅当$G^{(1)} = 1$，归纳地定义$G^{(n)} = G^{(1)(n-1)}$，于是有下列命题

命题41.2. *群G可解当且仅当存在r满足$G^{(r)} = 1$*

证明：充分性。此时G有现成的次正规列

$$1 = G^{(r)} \lhd G^{(r-1)} \lhd \cdots \lhd G^{(1)} \lhd G^{(0)} = G$$

每个商群都是abel的。再证必要性。设有次正规列

$$1 = G_r \lhd G_{r-1} \lhd \cdots \lhd G_1 \lhd G_0 = G$$

使得每个商群都是abel的。由G/G_1是abel的知$G^{(1)} < G_1$，$G^{(2)} = G^{(1)(1)} < G_1^{(1)} < G_2$，最后一步用到了$G_1/G_2$是abel的，归纳可得$G^{(r)} < G_r = 1$。

这个命题有简单推论：

可解群的子群、商群可解。

现在集中研究有限群。显然任意有限群G有不可加细的次正规列

$$1 = G_n \lhd G_{n-1} \lhd \cdots \lhd G_1 \lhd G_0 = G$$

即每个商群$G_i/G_{i+1}, i = 0, ..., n-1$都是单群，我们称这样的次正规列为合成列。不过合成列一般不唯一，但有幸的是一个定理（Jordan-Holder-赵强）保证对任何合成列，那些商群$G_i/G_{i+1}, i = 0, ..., n-1$在同构意义下，不计顺序，要记出现的次数都是相同的，换句话说，这些商群只取决于G，称之为G的因子群。于是有限群的分类问题分解为以下两个问题：

1) 给定G的因子群后的G的分类，即如何由G的因子群描述G；

2) 有限单群的分类。

1)就是群的扩张理论，并未完成；2)是完全解决。有一个有限单群分类定理（大定理，Fields获奖工作）将有限单群分成四个大类和26个例外的群。其中两个简单的类是

I. 素数阶群。

II. 交错群A_n（n元偶置换的群），$n \geq 5$。

注：I就是有限交换单群，由命题6.2.1刻画；II将作为本课的大定理之一在以后证明。整个有限单群分类定理不可能证明，作为常识，记住证明过程中的一个关键定理是

奇数阶群可解。

最后是三个Sylow定理，Sylow第一定理是说有限群的素数幂阶子群的存在性，这是拉格朗日定理的部分逆；Sylow第一定理是对这些子群的相互关系及个数的进一步描述。Sylow定理证明的主要工具是群在集合上的作用。当然群在集合上的作用绝不仅是用来证明Sylow定理，而是非常重要的数学工具（不限于代数领域）。

42 Jordan-Holder定理

现在来证明本课中群论部分的第一个大定理——Jordan-Holder定理

定理42.1. （*Jordan-Holder*）有限群G的任意两个无重复项的合成列有相同的长度，而且它们的因子群在同构意义下不计次序（记出现次数）相等。

证明：对群的阶做归纳。1阶、2阶显然成立。现设对阶小于$|G|$的群已成立。并设没有重复项的合成列如下：

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_r = 1 \tag{1}$$

$$G = H_0 \triangleright H_1 \triangleright \cdots \triangleright G_s = 1 \tag{2}$$

先按G_1是否$=H_1$分两种情形：
1) $G_1 = H_1$;
此时当然有$G/G_1 = G/H_1$，但因$G_1 \subsetneq G$，故由归纳假设知$G_1 = H_1$的两个合成列

$$G_1 \triangleright \cdots \triangleright G_r = 1$$

$$H_1 \triangleright \cdots \triangleright G_s = 1$$

有相同的长度和因子群，因此原来两个合成列也有相同的长度和因子群；
2) $G_1 \neq H_1$;
首先G_1与H_1必无包含关系（否则与G/G_1和G/H_1是单群矛盾），那么$G_1H_1 \supsetneq G_1$，由G/G_1是单群，知$G_1H_1 = G$。由同构定理知：

$$G/G_1 = G_1H_1/G_1 \cong H_1/G_1 \cap H_1$$

$$G/H_1 = G_1H_1/H_1 \cong G_1/G_1 \cap H_1$$

将次正规列

$$G \triangleright G_1 \triangleright G_1 \cap H_1$$

$$G \triangleright H_1 \triangleright G_1 \cap H_1$$

分别扩充成合成列

$$G = G_0 \triangleright G_1 \triangleright G_1 \cap H_1 := N_2 \triangleright \cdots \triangleright N_m = 1 \tag{3}$$

$$G = H_0 \triangleright H_1 \triangleright G_1 \cap H_1 := N_2 \triangleright \cdots \triangleright N_n = 1 \tag{4}$$

由上述同构关系知(3)和(4)有相同的长度和因子群；但由情形1)知(1)和(3)、(2)和(4)有相同的长度和因子群。因此(1)和(2)有相同的长度和因子群。

43 群的直和

由两个群G_1, G_2构造一个新的群，其实它也是群G_1, G_2的一种特殊的扩张，方法如下：做笛卡尔乘积$G_1 \times G_2$，按分量定义运算得到一个群。这个群称为G_1与G_2的（外）直和，这里的“外”指的是从集合上，G_1与G_2不是G的子集。但它们分别到$G_1 \times G_2$有单同态：

$$g_1 \longmapsto (g_1, e_2),\ \ g_2 \longmapsto (e_1, g_2)$$

其像G_1'与G_2'则分别是它们的“影子”（只要你愿意，可以不区别），作为$G_1 \times G_2$的子群，G_1'与G_2'满足以下三条性质：

1) $G_i' \triangleleft G_1 \times G_2, i = 1, 2$

2) $G_1' G_2' = G_1 \times G_2$

3) $G_1' \cap G_2' = (e_1, e_2)$。

2)和3)一起给出$G_1 \times G_2$到$G_1' \times G_2'$的双射，1)保证这是同构。我们可以说$G_1 \times G_2$

综上有如下结论：

群$G \cong G_1 \times G_2 \Longleftrightarrow$当且仅当存在$G$的分别同构于$G_1$和$G_2$的子群$G_1'$和$G_2'$，满足以下三条性质：

1) $G_i' \triangleleft G, i = 1, 2$

2) $G_1' G_2' = G$

3) $G_1' \cap G_2' =$空集。

我们可以说G是G_1'与G_2'的（内）直和，这里的“内”指的是G_1'与G_2'是G的子集。记为

$$G_1' \oplus G_2'$$

前面的结论实际是说内外直和本质相同，以后看到

$$G = G_1 \oplus G_2$$

可以指内外直和，就看G_1与G_2是否G的子群。最重要的是迅速翻译内外只和。一般地，两个群构造新的群用外直和，将一个大群分解为子群的直和用内直和。例如：用外直和可得群$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$；对用乘法表给出的Klein群$G = \{e, a, b, c\}$，可以取子群$G_1 = e, a, G_2 = e, b$，验证有内外直和关系

$$G = G_1 \oplus G_2 \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$$

直和可以由两个群推广到任意有限个群，细节自己补充。

44 有限生成abel群的结构定理

定理44.1. 对任何有限生成*abel*群M，存在唯一的非负整数r，m，和m个大于*1*的整数$d_1|d_2|\cdots|d_m$，使得

$$M \cong \mathbb{Z}^r \oplus \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_m\mathbb{Z}$$

注：若$r=0$，则前面部分$\mathbb{Z}^r$消失，若$m=0$，则后面部分消失。因为这里关心的是分类，所以有外直和，意味着一个有限生成abel群对应一组数据$(r,m,d_1,...,d_m)$。用内直和的语言，就是存在M中若干（可以是0）个无限阶元$\alpha_1,...,\alpha_r$，和若干（可以是0）个阶数有整除关系的有限阶元$\beta_1,...,\beta_m$，满足

$$M = \mathbb{Z}\alpha_1 \oplus \cdots \mathbb{Z}\alpha_r \oplus \mathbb{Z}\beta_1 \oplus \cdots \oplus \mathbb{Z}\beta_m$$

定理赏析：如何找出尽可能多（最好是全部）的有限生成abel群?首先想到由一个元生成的，那就是无限循环群$\mathbb{Z}$和有限循环群$\mathbb{Z}/n\mathbb{Z}$，然后想到把有限个循环群做直和。定理告诉我们这样已经给出了全部，并且有限群部分还有某种标准表示法使得唯一性成立。

例：$\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/15\mathbb{Z}$ （用孙子定理）

$\mathbb{Z}/45\mathbb{Z} \oplus \mathbb{Z}/75\mathbb{Z} \cong \mathbb{Z}/15\mathbb{Z} \oplus \mathbb{Z}/9\times 25\mathbb{Z}$ （反复用孙子定理）

与循环群类似，我们有：n个元生成的abel群同构于$\mathbb{Z}^n$的商，于是研究有限生成abel群的分类就是分类$\mathbb{Z}^n$的商。先对$\mathbb{Z}^n$做一些描述。

- **有限生成的自由abel群**。同构于某个$\mathbb{Z}^n$的群称为有限生成的自由abel群，n称为群的秩。
- **基**。若群abel$G$中有元素$e_1,...,e_n$满足

1) $G = \mathbb{Z}e_1 + \cdots + \mathbb{Z}e_n$

2) $a_1e_1 + \cdots + a_ne_n = 0 \Longleftrightarrow a_1 = \cdots = a_n = 0$,

则称$e_1,...,e_n$为G的一组基。

基也可等价地描述为$G = \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_n$且每个$e_i$是无限阶。

显然一个群有这样一组基等价于这个同构于$\mathbb{Z}^n$。注意：一旦有基，就会有大量的基，给一组基就是给一种同构于$\mathbb{Z}^n$的方式。

现在我们有定理证明的方案如下：

1. 证明有限生成abel群同构于有限生成自由abel群的商。

这一步的证明只需同态基本定理，完全平行于研究循环群的方法。第一步把问题化为分类有限生成自由abel群的商。

2. 研究有限生成自由abel群的子群的结构，有下列结论:

秩为n的自由abel群的子群一定是秩$\leq n$的自由abel群

应注意的是真子群的秩可以为n，自己举例。这一步的证明需用到下列引理：

（钟无倦）设G是abel群，若有$H < G$，使得H和G/H分别是秩为m和n的自由abel群，则G是秩为$m+n$的自由abel群。

3. 设G是秩为n的自由abel群，对什么特殊的子群H，G/H的结构简单、清晰？

有如下命题：

（王玖玮）若abel群G有一组基$e_1,...,e_n$，子群H有一组基$d_1e_1,...,d_me_m$，$m \leq n$，则

$$G/H \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_m\mathbb{Z} \oplus \mathbb{Z}^{n-m}$$

4. 证明3中的特殊情形并不特殊，原因是基是很多的，对任意H，可选择你需要的（G和H的）基。

1）（郭汝驰）若$e_1,...,e_n$是abel群G的基，则对任意矩阵$A\in GL(n,\mathbb{Z})$，$(e_1',...,e_n')=(e_1,...,e_n)A$也是基，并且这给出了全部基

2）（钟友林）设G是秩为n的自由abel群，H是秩为m的子群，则存在G的一组基$e_1,...,e_n$和子群H的一组基$d_1e_1,...,d_me_m$，且$d_1|\cdots|d_m$

45 “存在性部分”证明

1、归结为自由abel群的商。

设M是由n个元$\alpha_1,...,\alpha_n$生成的abel群，定义$\mathbb{Z}^n$到M的同态

$$\phi:(a_1,...,a_n)\longmapsto a_1\alpha_1+\cdots+a_n\alpha_n$$

它当然是满同态，由同态基本定理知道

$$M\cong\mathbb{Z}^n/\mathrm{Ker}\phi$$

于是分类M变成了分类$\mathbb{Z}^n$的各种商群。

2、对$\mathbb{Z}^n$的特殊子群做商，具体说证明对以$e_1,...,e_n$为基的自由abel群G和以$\varepsilon_1=d_1e_1,...,d_me_m$，$m\le n$为基的子群$H$，必有

$$G/H\cong\mathbb{Z}/d_1\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}/d_m\mathbb{Z}\oplus\mathbb{Z}^{n-m}$$

这一步的证明仍然只需同态基本定理。只要做G到$\mathbb{Z}/d_1\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}/d_m\mathbb{Z}\oplus\mathbb{Z}^{n-m}$的映射

$$d_1e_1+\cdots+d_ne_n\longmapsto(\overline{d_1},...,\overline{d_m},d_{m+1},...,d_n)$$

经检查，它是满同态且以H作为核。

3、证明一般情形可以约化到上述情形，并且可以进一步要求$d_1,...d_n$有整除关系。

(1) 证明（秩有限的）自由abel群的子群也自由，且秩不超过原来的群的秩。（做约定，0元构成的群也称自由，秩为0）

这里需要一个引理

引理45.1. *若abel群G有子群H使得，H和G/H是自由的，秩分别为m和n，则G是秩为$m+n$的自由abel群。*

证明：设$e_1,...,e_m$是H的基，$\overline{\varepsilon_1},...,\varepsilon_n$是$G/H$的基，我们来证明$e_1,...,e_m,\varepsilon_1,...,\varepsilon_n$正好是$G$的基。首先证明是生成元：对任意$x\in G$，由$\overline{\varepsilon_1},...,\varepsilon_n$是$G/H$的基知存在整数$b_1,...,b_n$满足

$$\overline{x}=b_1\overline{\varepsilon_1}+\cdots+b_n\overline{\varepsilon_n}=\overline{b_1\varepsilon_1+\cdots+b_n\varepsilon_n}$$

即$x=h+b_1\varepsilon_1+\cdots+b_n\varepsilon_n,h\in H$，再利用$e_1,...,e_m$是$H$的基可知

$$x=a_1e_1+\cdots+a_me_m+b_1\varepsilon_1+\cdots+b_n\varepsilon_n$$

再证明$e_1,...,e_m,\varepsilon_1,...,\varepsilon_n$线性无关：设有整数$a_1,...,a_m,b_1,...,b_n$满足

$$a_1e_1+\cdots+a_me_m+b_1\varepsilon_1+\cdots+b_n\varepsilon_n=0$$

放入商群中有

$$b_1\overline{\varepsilon_1}+\cdots+b_n\overline{\varepsilon_n}=\overline{0}$$

由$\overline{\varepsilon_1},...,\overline{\varepsilon_n}$是$G/H$的基知$b_1=\cdots=b_n=0$，于是

$$a_1e_1+\cdots+a_me_m=0,$$

再利用$e_1,...,e_m$是H的基可知每个$a_i=0$。

这就证明了引理，这个引理结合1实际上告诉我们

一个abel群是有限生成自由的当且仅当存在一个子群使得子群和商群都是有限生成自由的，且它们的秩有和关系。

现在可以证明(1) 设M是秩为n的自由abel群，对M的秩做归纳，$n=1$时以前已经知道子群的结构，确实是秩不超过1的自由abel群。现设$n>1$，且结论对秩$<n$的群已经成立。先取M的一个特殊的子群H使得H和M/H都自由，且秩都严格>0和$<n$ （只需将M的一组基分成两块即可），现设G是M的任意子群，那么$G\cap H<H$，由归纳假设知

$G\cap H$**是自由的。**

此外，$G/G\cap H\cong G+H/H<M/H$，再用归纳假设知

$G/G\cap H$**是自由的。**

上述两段黑体结合引理知G自由且秩不超过n。

(2)证明若abel群M有一组基$e_1,...,e_n$，则M有大量基，且全部基是：

$$(\varepsilon_1,...,\varepsilon_n)=(e_1,...,e_n)A,A\text{跑遍}GL(n,\mathbb{Z})$$

首先由$e_1,...,e_n$是基知任一组元$\varepsilon_1,...,\varepsilon_n$必可唯一表为上式，不过只能保证$A\in M_n(\mathbb{Z})$。需要说明

$\varepsilon_1,...,\varepsilon_n$**是基，当且仅当**$A$**可逆**

先证必要性：由于$\varepsilon_1,...,\varepsilon_n$是基，有矩阵$B\in M_n(\mathbb{Z})$使得

$$(e_1,...,e_n)=(\varepsilon_1,...,\varepsilon_n)B$$

故

$$(e_1,...,e_n)=(e_1,...,e_n)AB$$

从而$AB=I_n$，即$A\in GL(n,\mathbb{Z})$。

再证充分性：取行向量$X\in\mathbb{Z}^n$，使得$(\varepsilon_1,...,\varepsilon_n)=0$，即

$$(e_1,...,e_n)AX=0$$

而$e_1,...,e_n$是基，故$AX=0$，从而$X=0$，即$\varepsilon_1,...,\varepsilon_n$是基。

(3) 设M是秩为n的自由abel群，$N<M$是秩为m的子群，则存在M的一组基$e_1,...,e_n$，和N的一组基$d_1e_1,...,d_me_m$，且有$d_1|\cdots|d_m$.

首先任取M和N的各一组基$e_1',...,e_n'$和$\varepsilon_1',...,\varepsilon_m'$，则有整数矩阵$A$满足

$$(\varepsilon_1',...,\varepsilon_m')=(e_1',...,e_n')A$$

由(2)知只要取矩阵$P\in GL(n,\mathbb{Z}),Q\in GL(m,\mathbb{Z})$，我们可得到$M$和$N$的另外各一组基$e_1,...,e_n$和$\varepsilon_1,...,\varepsilon_m$满足

$$(e_1,...,e_n)=(e_1',...,e_n')P$$

$$(\varepsilon_1,...,\varepsilon_m)=(\varepsilon_1',...,\varepsilon_m')Q$$

综合各式有

$$(\varepsilon_1,...,\varepsilon_m)=(e_1,...,e_n)P^{-1}AQ$$

我们需要的变成寻找适当可逆矩阵P、Q使得$P^{-1}AQ$成为对角形，且元素有整除关系。这归结为如下引理：

引理45.2. *对任何$n\times m$整数矩阵A，存在可逆方阵P、Q使得PAQ成为成为对角形，且元素有整除关系。*

证明：先定义三类初等行（列）变换：

(1) 将矩阵的某一行（或列）乘以一个$\mathbb{Z}$的单位，即±1
(2) 将两行（或列）交换
(3) 将某一行（或列）乘以一个元素加到另一行（或列）上

与一般线性代数中一样，做一个初等行（列）变换等于左（右）乘相应的初等矩阵，因此只需证任意矩阵可经过有限步初等变换化成标准形。在$\mathbb{Z}$中引进偏序:若$0<|a|<|b|$，我们说$a<b$，再规定0是最大的；对矩阵A,B，也可按矩阵的元的最小者定义$A<B$。现分几步完成证明：

第一步。证明若非零矩阵A的某一最小元不整除其它某个元，则A等价于某一更小的矩阵:
首先，通过行列交换将A中最小的元移到第一行第一列，不妨设$A=(a_{ij})$，a_{11}是最小的。
第一种情形：若有某一$a_{i1}\not\equiv 0 \pmod{a_{11}}$，通过带余除法知可做初等行变换得到矩阵$(b_{ij})$，满足$b_{i1}<a_{i1}$;
第二种情形：若a_{11}整除第一行和第一列上所有的元，此时可设$a_{11}\nmid a_{ij}$，$i>1,j>1$。于是可将A变为$A'=(a'_{ij})$，其中$a'_{11}=a_{11}$，$a'_{i1}=a'_{1j}=0$。由于做这些变换时，所有元都保持$\mathrm{mod}a_{11}$不变，因此有$a'_{11}\nmid a'_{ij}$。将A'的第i行加到第一行上得到一个新的矩阵(c_{ij}),满足$c_{11}=a'_{11}=a_{11}$，但$c'_{11}\nmid c'_{ij}$，这就划归第一种情形。

第二步。证明非零矩阵A等价于如下形状的矩阵

$$\begin{pmatrix} a_1 & 0 \\ 0 & A_1 \end{pmatrix},$$

这里$a_1\in R,A_1$是$n-1$阶方阵，且a_1整除A_1的所有元。
因为不能有无限长的矩阵列

$$C_1>C_2>\cdots,$$

故由第一步的结论知A可化为$B=(b_{ij})$，它满足：B的最小元整除其它所有元，不妨设b_{11}就是最小元，它整除任何b_{ij}，于是可做（第3类）初等行列变换将B变成第一行和第一列上所有的元都是0的矩阵，同样地在变换中所有的元素都保持$\mathrm{mod}a_{11}$不变，故变成了我们需要的形状

通过前两步知对n做归纳可得结论。

练习。
1、将自然的同构$\mathbb{Z}/15\mathbb{Z}\cong\mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/5\mathbb{Z}$ 翻译为内直和，即找出$\mathbb{Z}/15\mathbb{Z}$的两个相应的子群。
2、设G是有限生成abel群。证明
（1）G有限 $\Longleftrightarrow$ G的每个元的阶有限, $\Longleftrightarrow$ G的一组生成元的阶有限
（2）对任意正整数n，群G/nG有限。

（3）G自由 $\Longleftrightarrow$ G的每个非0元的阶无限，
（4）G的所有有限阶元形成子群。问所有无限阶元连同0是否形成子群？
3、设群G同构于$\mathbb{Z}\oplus\mathbb{Z}/n\mathbb{Z}$，问
（1）同构$\phi:\mathbb{Z}\oplus\mathbb{Z}/n\mathbb{Z}\longrightarrow G$有几个？
（2）取$\mathbb{Z}\oplus\mathbb{Z}/n\mathbb{Z}$的子群

$$A=\{(a,\overline{0})|a\in\mathbb{Z}\},B=\{(0,\overline{b})|b\in\mathbb{Z}\},$$

当ϕ取遍上述同构时，共有多少个$\phi(A)$和$\phi(B)$。
4、设有群G_1,G_2，分别有正规子群H_1,H_2，证明

$$G_1\times G_2/H_1\times H_2\cong G_1/H_1\times G_2/H_2$$

5、证明：
1) 若有群同构$\phi:G\longrightarrow G'$，H是G的正规子群，则$G/H\cong G'/\phi(H)$
2) 若G交换，运算记为加法，则$G/pG\cong G'/pG'$
3) 若有群G同构于G'，G的正规子群H同构于G'的正规子群H'，能否保证$G/H\cong G'/H'$?
6、设$G=\mathbb{Z}/p^n\mathbb{Z}$，$n>1$，证明$G/pG\cong\mathbb{Z}/p\mathbb{Z}$.
7、设有素数p和正整数$a_1,...,a_m$。证明：若有群同构

$$G\cong\mathbb{Z}/p^{a_1}\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}/p^{a_m}\mathbb{Z}$$

则m是G的同构不变量（提示，对任意加法群G，考察G/pG）。
8、设有群M同构于

$$\mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/5\mathbb{Z}\oplus\mathbb{Z}/25\mathbb{Z},$$

（1）定理中的$r,m,d_1,...,d_m$各是多少？
（2）取$\mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/5\mathbb{Z}\oplus\mathbb{Z}/25\mathbb{Z}$的子群

$$A=\{(\overline{a},\overline{0},\overline{0},\overline{0})|a\in\overline{Z}\},\ \ B=\{(\overline{0},\overline{b},\overline{0},\overline{0})|b\in\overline{Z}\}$$

$$C=\{(\overline{0},\overline{0},\overline{c},\overline{0})|c\in\overline{Z}\},\ \ D=\{(\overline{0},\overline{0},\overline{0},\overline{d})|d\in\overline{Z}\}$$

请问同构$\phi:\mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/5\mathbb{Z}\oplus\mathbb{Z}/25\mathbb{Z}\longrightarrow M$有几个？所有的$\phi(A),\phi(A+B),\phi(C),\phi(D)$各有多少个？
9、我们称上题的m为G的长度。现有群$G=\mathbb{Z}/p\mathbb{Z}\oplus\mathbb{Z}/p^3\mathbb{Z}\oplus\mathbb{Z}/p^3\mathbb{Z}\oplus\mathbb{Z}/p^6\mathbb{Z}\oplus\mathbb{Z}/p^6\mathbb{Z}\oplus\mathbb{Z}/p^6\mathbb{Z}$，对非负整数$n$，讨论群$p^nG$的长度。
10、设G是27×25阶可解群，它的因子群有那些？
11、设G是秩为n的自由abel群，证明：
(1) G中n个元若能生成G，则它是G的基；
(2) G到自己的满同态必为同构。

第十四周 有限生成abel群续

46 唯一性部分

我们需要证明对任意有限生成abel群M，当它满足定理的形式

$$M\cong\mathbb{Z}^r\oplus\mathbb{Z}/d_1\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}/d_m\mathbb{Z}\qquad(1),$$

时，各个量$r, d_1, ..., d_m$都是M的（同构）不变量。首先将(1)写成内直和形式：
$M = M_1 \oplus M_2$，
$M_1 \cong \mathbb{Z}^r$，
$M_2 \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_m\mathbb{Z}$
注意：
a) M_1中的非0元全是无限阶的，而M_2中的元全是有限阶的；
b) 有限阶元+无限阶元=无限阶元
因此M_2正好是M的有限阶元之集合，我们记它为M_{tor}。以下按步骤进行。

1、将问题简化到有限群的情形。

前面的观察知(1)式意味着

$$M_{tor} \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_m\mathbb{Z}$$

$$M/M_{tor} \cong \mathbb{Z}^r$$

（显然，M的同构类决定M_{tor}和M/M_{tor}的同构类）两式中后一个意味着r的确是M的（同构）不变量。前一个则意味着剩下只需证定理对有限群成立。

2、将问题简化到有限p-群的情形。

若M有限，设M的阶为n。再设

$$M \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_m\mathbb{Z} \tag{2},$$

由孙子定理，我们知道每个$\mathbb{Z}/d_i\mathbb{Z}$同构于若干个阶为素数幂（d_i的素数幂因子）的循环群的直和，这样M也同构于阶为素数幂（所有d_i的所有素数幂因子）的循环群的直和，而且$d_i, i = 1, ..., m$的素数幂因子的全体（称为$d_i, i = 1, ..., m$的初等因子）与d_i的全体可以互相决定，因此我们只需说明M和(2)式能决定d_i的全体初等因子即可。设全体初等因子为

$$p^{a_{1,p}}, ..., p^{a_{r_p,p}}, p\text{跑遍}n\text{的素因子}$$

则有

$$M \cong \oplus_{p|n}(\mathbb{Z}/p^{a_{1,p}}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{a_{r_p,p}}\mathbb{Z})$$

写成内直和有

$$M = \oplus_{p|n} M_p \tag{3}$$

$$M_p \cong \mathbb{Z}/p^{a_{1,p}}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{a_{r_p,p}}\mathbb{Z} \tag{4}$$

但上两式意味着：

$$M_p = M\text{的阶为}p\text{的幂的元形成的子群。}$$

具体说，任一$x \in M$可唯一表为$\sum_p x_p, x_p \in M_p$，而x的阶是所有x_p的阶之积。

注意M_p是不依赖于分解方法的。如果能证明M_p和(4)式能决定所有$p^{a_{i,p}}$，就能说明M和(2)式能决定所有d_i。这样我们就将定理归结为了有限p-群的情形。

3、对有限p-群M证明定理。

要证明由有限p-群M和同构

$$M \cong \mathbb{Z}/p^{a_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{a_m}\mathbb{Z}, 0 < a_1 \leq \cdots \leq a_m$$

能完全决定每个a_i。首先说明M能完全决定m，反复用同态基本定理可得

$$M/pM \cong \mathbb{Z}/p\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p\mathbb{Z}(m\text{个})$$

我们暂时引进术语：称上述同构决定的m为M的长度。

现将M重新表示为$M \cong M_1 \oplus \cdots \oplus M_n$，而每个$M_i$是$n_i$个$\mathbb{Z}/p^{b_i}\mathbb{Z}$的直和，$b_1 > \cdots > b_n$。现在把每个量$b_i, n_i$都用$M$内在地描述，从而完成最后证明。考察模$p^r M$，让$r$从充分大开始递减地变化，那么我们有：

(a) $b_1 - 1$是第一个使$p^r M$非零的r，而n_1正是这个$p^r M$的长度；

(b) $b_2 - 1$是继$b_1 - 1$之后第一次使$p^r M$的长度发生变化的r，而n_2正是这个$p^r M$的长度增加的数目。以此类推可知每个量b_i, n_i都是M的不变量。

证明完了整个定理之后，我们可以将r称为M的秩，$d_1, ..., d_m$称为M的不变因子，那些素数幂因子称为M的初等因子。而将M_p称为M的p分支。

47 例子

例1、$(\mathbb{Z}/n\mathbb{Z})^\times$是一类典型的有限生成abel群。

$$(\mathbb{Z}/2^m\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2^{m-2}\mathbb{Z}, m \geq 2$$

$$(\mathbb{Z}/5^2 \times 13\mathbb{Z})^\times \cong (\mathbb{Z}/5^2\mathbb{Z})^\times \oplus (\mathbb{Z}/13\mathbb{Z})^\times \cong \mathbb{Z}/(5 \times 4)\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$$

重新整理为

$$(\mathbb{Z}/5^2 \times 13\mathbb{Z})^\times \cong \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/(3 \times 4 \times 5)\mathbb{Z}$$

$(\mathbb{Z}/65\mathbb{Z})^\times$的不变因子是4和60；初等因子是4，4，3，5.

例2、考察曲线$E : \{(x, y) \in \mathbb{C}^2 | y^2 = x^3 + ax + b\} \bigcup \{O\}, a, b \in \mathbb{Q}, 4a^3 + 27b^2 \neq 0.$

点O称为无穷远点（可以看作人为添加的点，实际上有含义），条件$4a^3 + 27b^2 \neq 0$保证多项式$x^3 + ax + b$无重根，即曲线上没有奇点。这样的E称为定义在$\mathbb{Q}$上的椭圆曲线。对$\mathbb{C}$的任何子域F，可以有F点集合

$$E(F) : \{(x, y) \in F^2 | y^2 = x^3 + ax + b\} \bigcup \{O\}$$

在$E(F)$上可以定义一个加法运算使之成为abel群：

1）$P + O = O + P = P$

2）若P和Q关于X轴对称，则$P + Q = O$

3）若非上述情形，连接PQ（$P = Q$时，引切线）交E于另一点R，作R关于X轴的对称点S，则$P + Q = S$

可以检查（不显然）这样的加法有结合律，进一步，这些点构成一个加法群（显然），群的单位元就是那个无穷远点，一个点的逆元则是它关于X轴的对称点。所有有理点的集合也构成群。

我们最关心群$E(\mathbb{Q})$，要完全弄清楚它是很难的，但我们知道：

（Mordell定理）$E(\mathbb{Q})$是有限生成的abel群。

还有一个更不可思议的定理说$E(\mathbb{Q})_{tor}$的结构只有有限种可能。

（Mazur定理）$E(\mathbb{Q})_{tor}$同构于下列群之一：

$\mathbb{Z}/m\mathbb{Z}, m = 1, 2, 3, ..., 10, 12$

$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}, m = 2, 4, 6, 8$

困难的是$E(\mathbb{Q})$的秩r。著名的BSD猜想（美国Clay研究所悬赏100万美元的七个千禧年难题之一）说r应等于某一个由E定义的复解析函数$L_E(s)$在特殊点$s = 1$处的阶。$L_E(s)$现在无法给出定义，但需要说明的是它是一个定义复杂却可以计算的对象；反过来r 是定义简单却难以计算的量。BSD猜想在古老的（至少千岁）同余数问题上有简单应用。称正整数n是同余数，如果n是三边都是有理数的直角三角形的面积（等价地可描述为n是三个成等差数列的平方数的公差）。对奇数n，BSD猜想预言下列两条等价：

1) 奇数n是同余数；

2) 方程$x^2 + 2y^2 + 8z^2 = n$的整数解中z为奇、偶的各占一半。

一个Coates-Wiles定理回答了BSD猜想中的小部分，但足以保证上述两条的1) $\Rightarrow$ 2)。

练习。

1、写出群$(\mathbb{Z}/5^2 \times 7^2 \times 13\mathbb{Z})^\times$的全体初等因子和不变因子。

2、因子群为$\mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/5\mathbb{Z}, \mathbb{Z}/5\mathbb{Z}, \mathbb{Z}/5\mathbb{Z}$ 的abel群有多少个同构类？

3、证明：若有群同构$\phi : G \longrightarrow G'$，和子群$H \lhd G$，则$G/H \cong G'/\phi(H)$。请在有限abel群范围内举例说明$G \cong G', H(< G) \cong H'(< G')$不能保证$G/H \cong G'/H$。

4、自然地定义加法群中$\mathbb{Z}$线性相关和秩的概念，证明群$\mathbb{Q}$的性质：

1) 秩为1

2) 任何有限生成的子群都是循环群，

3) 非有限生成。

5、对abel群G和正整数n，引进记号$G[n] := \{x \in G | nx = 0\}$，$[n] : G \longrightarrow G, x \longmapsto nx$。证明：若对任意$n$，均有

1) $|G[n]| = n^2$，

2) 映射$[n]$是满的

则

$$G[n] \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$$

48 对称群S_n

n个数$1, 2, ..., n$的所有置换按映射的合成形成的群称为n元对称群，记为S_n。显然任何n元集合X的对称群$S(X)$也与它同构，由Cayley定理知任何有限群都同构于某一S_n的子群。看基本概念：

- **轮换** S_n中元素$(i_1...i_s)$：将i_1映到i_2，i_2映到i_3，以此类推，最后i_s映到i_1，保持其它的元不变。
- **对换** 两个元组成的轮换(ij)。
- **不动点** $\sigma \in S_n$的不动点指的是满足$\sigma(x) = x$的x。

基本性质：

1. 任何置换都可表为有限个对换之积。

2. 对任何$\sigma \in S_n$，有

$$\sigma(i_1...i_s)\sigma^{-1} = (j_1...j_s), j_1 = \sigma(i_1), ..., j_s = \sigma(i_s)$$

3. 任意置换都可唯一地（不计顺序）表为不交的轮换之积。

1.是平凡的。2容易证明，但需理解清楚：对一个n元集合X，如何给出S_n到$S(X)$的同构？自然的想法是先给集合X一个编号，即给一个双射$\phi : \{1, 2, ..., n\} \longrightarrow X$，然后通过下列交换图给出同构$\widehat{\phi} : S_n \longrightarrow S(X)$

$$\begin{array}{ccc} \{1,2,...,n\} & \xrightarrow{\phi} & X \\ {\scriptstyle\tau}\downarrow & & \downarrow{\scriptstyle\widehat{\phi}(\tau)} \\ \{1,2,...,n\} & \xrightarrow{\phi} & X \end{array}$$

但编号的方法并非唯一，甚至没有一个最好的，即对任意的$\sigma \in S_n$，可以用$\phi \circ \sigma$重新编号，即有下图

$$\begin{array}{ccccc} \{1,2,...,n\} & \xrightarrow{\sigma} & \{1,2,...,n\} & \xrightarrow{\phi} & X \\ {\scriptstyle\tau}\downarrow & & {\scriptstyle\tau'}\downarrow & & \downarrow{\scriptstyle\widehat{\phi}(\tau')} \\ \{1,2,...,n\} & \xrightarrow{\sigma} & \{1,2,...,n\} & \xrightarrow{\phi} & X \end{array}$$

此时中间的箭头τ'就是$\sigma\tau\sigma^{-1}$。所以$\sigma\tau\sigma^{-1}$与τ只差一个编号，具有完全相同的形状。

现在简单证明3：任取$\tau \in S_n$，可在集合$\{1, 2, ..., n\}$上定义等价关系$\sim$如下：

$$x \sim y \Longleftrightarrow \text{存在正整数}r\text{满足}y = \tau^r(x)$$

（自己验证它是等价关系，注意τ是有限阶的。）得到$\{1, 2, ..., n\}$的一个划分$A_1 \cup A_2 \cup \cdots \cup A_s$。任取$a_i \in A_i$，记$r_i$为满足$\tau^r(a_i) = a_i$的最小$r$，那么$r_i$正好是$A_i$的元素个数，且$A_i = \{\tau^i(a_i) | i = 0, 1, ..., r_i - 1\}$。那么$\tau|_{A_i}$正好是这$r_i$个元的轮换。从而$\tau$是所有这些由划分决定的轮换之积。

以下关于运算的简单性质也很常用：

4. $(i_1 \cdots i_{s+t}) = (i_1 \cdots i_s)(i_s i_{s+1} \cdots i_{s+t})$

因此有$(12\cdots n) = (n12\cdots, (n-1)) = (1n)(12\cdots(n-1))$=$(1n)(1, n-1)\cdots(12)$

5. 对任意$x \in \{1, 2, ..., n\}$，以x为不定点的τ的全体形成子群。

6. 奇数个对换之积一定非平凡。

性质6虽然是熟知的，但并非天经地义，而是一条需证明的性质。证明：对乘积中对换个数做归纳。假设个数小于奇数m的对换之积非平凡，现有m个对换之积τ，不妨设有一个对换含1，通过适当顺序调整，使得含1的对换全部在前面，即

$$\tau = \tau_1\tau_2, \tau_1 = (1i_1)\cdots(1i_s), \sigma_1\cdots\sigma_t, s + t = m, \text{每个}\sigma_i\text{是不含2的对换}$$

这样的调整能实现是因为等式$(23)(12) = (13)(23)$。先分两种情形：

1) $i_1, ..., i_s$中有重复。由性质2知τ_1可写成$s-2$个元之积，用归纳假设知τ非平凡。

2) $i_1, ..., i_s$中无重复。则$\tau_1(1) = i_s$，于是1是τ_2的不动点而非τ_1的不动点，当然非τ的不动点，故τ非平凡。

于是我们有奇置换和偶置换的概念。所有偶置换形成S_n的子群，称为交错群，记为A_n。它是指标为2的正规子群。

定理48.1. 对任何$n \geq 5$，A_n是单群。

在证明该定理之前，先给两个引理：

引理48.2. A_n由全体3轮换生成。

依定义，A_n有一组生成元：全体形如$(ab)(cd)$的元。这个引理是说生成元还可减少到全体(abc)，只需说明$(ab)(cd)$能有3轮换表出即可。这是显然的：$(12)(23)=(123),(12)(34)=(123)(234)$。

引理48.3. 对$n\geq 5$，任一3轮换(ijk)可表为$(ijk)=\sigma(123)\sigma^{-1}$，$\sigma\in A_n$。

证明：由性质2知(ijk)可表为$(ijk)=\sigma(123)\sigma^{-1}$，$\sigma\in S_n$，只要$\sigma(1)=i,\sigma(2)=j,\sigma(3)=k$，但$\sigma$和$\sigma(45)$都具有此性质，且必有一在$A_n$中。

定理6.9.1的证明思路：设H是A_n的阶>1的正规子群，需证明$H=A_n$，由引理6.9.2知只需证明H含有全体3轮换，再由引理6.9.3知只需证明H含有某一3轮换。注意；对非平凡置换τ，有

$$\tau\text{的不动点数}<n-1$$

$$\tau\text{是对换}\iff\tau\text{的不动点数是}n-2$$

$$\tau\text{是3轮换}\iff\tau\text{的不动点数是}n-3$$

因此我们的任务变为说明H中含有不动点数是$n-3$的元，即A_n中不动点数最多的非平凡元。因而化为证明如下断言：

任给H中不动点数$<n-3$的τ，就可找到非平凡$\tau'\in H$，使得τ'的不动点更多。

49 定理6.9.1的补证

定理6.9.1的证明:接前面的证明思路及记号，由于$H \triangleleft A_n$，故对任意$\sigma \in A_n$，有$\sigma\tau\sigma^{-1} \in H$。我们不能指望$\sigma\tau\sigma^{-1}$有更多的不动点（性质2），但只要$\sigma$的不动点多，会导致$\sigma\tau\sigma^{-1}$与$\tau$在很多点的取值相同，即$\tau' := \tau^{-1}\sigma\tau\sigma^{-1}$有很多不动点。因此取适当的3轮换$\sigma$可望完成任务。

我们知道：要使点x是$\tau^{-1}\sigma\tau\sigma^{-1}$不动的，只需（不必要）使$x$和$\tau(x)$都是$\sigma$不动的即可，因此我们应该尽力寻找$\sigma$使

1) τ不动点包含于σ不动点，从而也包含于$\tau^{-1}\sigma\tau\sigma^{-1}$不动点；

2) 某一个点x是τ的动点，但x和$\tau(x)$都是σ不动的，从而使x是$\tau^{-1}\sigma\tau\sigma^{-1}$不动的。

取$1 \neq \tau(1)$，设$\tau(1) = 2$，然后分$\tau(2)$是1和非1两种情形。若$\tau(2) = 3$，再选τ的另外两个动点$4, 5$（一定有！为什么？），取$\sigma = (345)$，它符合我们的要求，因此$\tau^{-1}\sigma\tau\sigma^{-1}$不动点更多，但它也非平凡（因为2是动点）；若$\tau(2) = 1$,且$\tau = (12)(34)\cdots$的因子中只有对换，取$\sigma = (345)$仍能完成任务，只是这时不是满足前面的两条，而是修正的以下两条

1') τ不动点去掉5以后包含于σ不动点，从而也包含于$\tau^{-1}\sigma\tau\sigma^{-1}$不动点；

2') 两个点1和2都符合2)的要求，从而是$\tau^{-1}\sigma\tau\sigma^{-1}$不动的。

综上，完成了定理证明（自己验证4是$\tau^{-1}\sigma\tau\sigma^{-1}$的动点）。

练习

1、对以下$\tau \in A_n$，找一个$\sigma \in A_n$，使得$\tau^{-1}\sigma\tau\sigma^{-1}$比$\tau$有更多的不动点：

（1）$\tau = (1234)(56) \in A_7$

（2）$\tau = (12)(34)(56) \in A_7$

2、代数学97页10-16题。

50 群作用基本知识

- 群G在集合X上的一个作用指的是一个映射$f : G \times X \longrightarrow X$，它满足如下性质：

$$1) \quad f(g_1, f(g_2, x)) = f(g_1g_2, x)$$

$$2) \quad f(e, x) = x$$

将$f(g, x)$记为$g(x)$，上述两式改写为：

$$1) \quad g_1(g_2(x)) = (g_1g_2)(x)$$

$$2) \quad e(x) = x$$

由这种写法可以看出群作用实际上是一个群同态$\phi : G \longrightarrow S(X)$。对任意$g \in G$，$\phi(g)$定义为$X$上映射$x \longmapsto g(x)$。由于1)和2)保证$\phi$是一半群同态，但$G$本身是群，故（自己推）$\phi(g)$总是可逆的。如果$\phi$单，则称作用是忠实的；如果对任意$g, x$，都有$g(x) = x$，则称它是平凡作用。

例1、群G作用在集合$X = G$上，作用定义为$g(x) = gx$。

例2、对任意子群$H < G$，有左陪集组成的集合$X = G/H$，G可以自然第作用于X上，作用定义为

$$g(aH) = gaH$$

例3、群G作用在集合$X=G$上，作用定义为$g(x)=gxg^{-1}$。这种作用称为共轭作用。

• **群作用的等价** G对X的作用ϕ等价于G对X'的作用ϕ'，指的是存在集合双射$\tau: X \longrightarrow X'$，满足对任意$g\in G$，下图交换：

$$\begin{array}{ccc} X & \xrightarrow{\tau} & X' \\ {\scriptstyle \phi(g)}\downarrow & & \downarrow{\scriptstyle \phi'(g)} \\ X & \xrightarrow{\tau} & X' \end{array}$$

• **齐性空间**：对群G的子群H，带有G的自然作用的集合G/H称为一个齐性空间。

• **轨道**：形如$O_x=G(x):=\{g(x)|g\in G\}$的集合称为一个轨道。

• **不动元**：$x\in X$称为G的不动元，如果对任意$g\in G$，都有$g(x)=x$，换句话说$O_x=\{x\}$。

• **稳定子群**：设G作用在X上，$x\in X$，x的稳定子群定义为$H_x=\{g\in G|g(x)=x\}$

• **传递的群作用**：称作用是传递的，如果只有一个轨道。

注：不同的轨道一定不交，而且群G可以自动作用在一个轨道或一些轨道之并上。G在X上的作用是传递的，等价于说X没有真子集能继承G在X上的作用。

命题50.1. 一个轨道等价于一个齐性空间

证明：设G作用在X上，$x\in X$，记x所在的轨道O_x，x的稳定子群H_x，做自然映射

$$\psi: G\longrightarrow O_x,\ g\longmapsto g(x)$$

它当然是满的，而且对任意$g\in G$，

$$\psi^{-1}(\psi(g))=gH_x$$

由集合映射的基本定理导出O_x与齐性空间G/H_x的一一对应。

对有限p-群作用在有限集上，可以有下列有趣的推论：

推论50.2. 设有限p-群G作用在有限集X上，如果t为X中不动元的个数，则

$$t\equiv |X| \pmod p$$

证明：首先X的任一轨道的元素个数都是$|G|$的因子，因而是p的幂，那么只能是1或p的倍数，进一步

$$O_x=\{x\}\Longleftrightarrow x\text{是不动元}$$

只要通过数各个轨道的方法数集合X，就有

$$t\equiv |X| \pmod p$$

推论50.3. 设有限p-群G作用在有限集X上，如果$|X|\not\equiv 0 \pmod p$，则X中一定有不动元。

将这些工具应用到例3，即有限群G对$X=G$的共轭作用，可以得到群的类方程，先引进几个概念：

给定群G和子集S，

• $Z(G):=\{x\in G|$对任何$g\in G$，有$gx=xg\}$称为群G的中心;

• $Z(S):=\{a\in G|a$与S中所有元可交换$\}$称为S的中心化子；

• $N(S):=\{a\in G|aS=Sa\}$称为S的正规化子；

由

$$X=\cup_{O_x}O_x=\text{不动元之集}\cup(\cup_{|O_x|>1}O_x)$$

数数得

$$|X| = \text{不动元数目} + \sum_{|H_x|<|G|} \frac{|G|}{|H_x|}$$

但$X = G$，不动元之集就是中心$Z(G)$，$H_x = Z(x)$，因此有

$$|G| = |Z(G)| + \sum_{|Z(x)|<|G|} \frac{|G|}{|Z(x)|}$$

这个等式称为群的类方程，它是极为重要的研究群的工具。先看一个简单应用。

命题50.4. 有限p-群必有非平凡中心

证明一：因$|G|$和每个$\frac{|G|}{|Z(x)|}$（当$|Z(x)| < |G|$时）都是p的正方幂，当然都是p的倍数，再由群的类方程知$p||Z(G)|$，但$|Z(G)| > 0$（单位元）。故$|Z(G)| \geq p$。
证明二：由于G共轭作用在G上时，有单轨道$\{e\}$，故可作用于$\{e\}$的补集X，而$|X| \equiv -1 \pmod{p}$，由推论立得还有不动元，即$Z(G)$中的非平凡元素。

推论50.5. 有限p-群必可解

证：对群的阶归纳，并利用中心非平凡立得。

推论50.6. p^2阶群必交换

证：仍然利用中心非平凡，细节自己补完整。

例4、三阶群G作用在集合$X = \{1, 2, 3, 4\}$上有几个作用？这些作用有几个等价类？

解：由推论知不动元数目为1或4。
1) 若不动元数目为4，则是平凡作用
2) 若不动元数目为1，则有两个轨道，一个是单轨道；另一个轨道含有三个元，等价于G对G的平移作用。

因此：所有作用有两类，共有$1 + 4 \times 2 = 9$个。

练习
1、对$\sigma = (124)(35) \in S_7$，考察$G = \langle\sigma\rangle$对集合$\{1, 2, 3, 4, 5, 6, 7\}$的自然作用，请
(1) 写出所有轨道。
(2) 写出在3和4处的稳定子群。
2、证明$Z(S_n) = \{(1)\}$
3、群S_3在集合$\{1, 2, 3\}$上可定义几个作用？等价类有几个？

51 Sylow定理

对有限群G和$|G|$的任意因子m，自然该问G的m阶群是否存在？一般并不对。Sylow第一定理告诉我们，当m是素数幂时是对的。

定理51.1. （*Sylow第一定理*）设G是有限群，$p^r||G|$，则存在G的p^r阶子群。

证明：对群的阶做归纳。一阶不需证，2阶显然成立。现设对阶小于$|G|$的群已经成立。分情形如下：
1）若$p||Z(G)|$，则abel群$Z(G)$有p阶子群K，当然有$K \triangleleft G$，考察G/K，它的阶满足：$p^{r-1}|\frac{|G|}{p} = |G/K|$，由归纳假设知$G/K$有$p^{r-1}$阶子群，设为$H/K$，必然$|H| = |K||H/K| = p^r$。
2）若p不整除$|Z(G)|$，则由群的类方程知存在$x \in G$满足

$$1 < \frac{|G|}{|Z(x)|} \not\equiv 0 \pmod{p}$$

故$p^r|Z(x)$，但$Z(x)$是G的真子群，由归纳假设知$Z(x)$有p^r阶子群，当然也是G的子群。

有限群G的子群H称为Sylow p-子群，如果$|H|$正好是$|G|$的p部分。Sylow第一定理告诉我们对$|G|$的任意素数幂因子p^r，存在p^r阶子群。进一步，该问这些子群有多少？有什么关系？显然任何p子群H，都有一些共轭子群gHg^{-1}与H有相同的阶。Sylow第二、第三定理会告诉我们Sylow p-子群在共轭意义下是唯一的，在通常意义下，个数是模p余1的，而且任意p-子群都含于一个Sylow p-子群中。

定理51.2. （*Sylow第二、三定理*）设G是有限群，X是G的所有*Sylow* p-子群之集，定义G在X上的共轭作用$g(H) = gHg^{-1}$，则
1) X只有一个G-轨道；
2) $|X| \equiv 1 \pmod{p}$
3) 任意p-子群含于一个*Sylow* p-子群中。

先证一个引理：

引理51.3. 设G是有限群，P是G的p-子群，K是一个*Sylow* p-子群，用$N(K) = \{g \in G|gKg^{-1} = K\}$表$K$的正规化子。若$P \subset N(K)$，则$P \subset K$

证明：由于$P < N(K)$，$K \triangleleft N(K)$，故$PK = KP$，因而PK是G的子群，而$|PK| = |P||K|/|P \cap K|$，故PK是p-子群，因此$|PK| \leq |K|$，但$PK \supset K$。故$K = PK \supset P$

定理证明：考察X的任一个非空的G作用下封闭的子集Y。我们来数一数Y，为此取G的p-子群P，它也作用在Y上。用$t_{P,Y}$表Y的P-不动元（即在P作用下不动的元）的个数。由推论6.11.2知

$$|Y| \equiv t_{P,Y} \pmod{p} \tag{1}$$

对任意$K \in Y$，明显地

$$K\text{是}P\text{-不动的} \iff P \subset N(K)$$

再由引理6.12.3知

$$K\text{是}P\text{不动的} \iff P \subset K \tag{2}$$

特别地若P是Sylow的p-子群，则(2)式变为

$$K\text{是}P\text{-不动的} \Longleftrightarrow P = K \tag{3}$$

分别取各种P完成我们的证明。
i) 取$P \in Y$，由(3)知Y有唯一P-不动元P，那么$t_{P,Y} = 1$。(1)式意味着

$$|Y| \equiv 1 \pmod{p} \tag{4}$$

ii) 假如$Y \subsetneq X$，可取$P \in X$，但$P \notin Y$，仍然由(3)式知，此时$t_{P,Y} = 0$，再由(1)式知

$$|Y| \equiv 0 \pmod{p}$$

从而与(4)式矛盾。由此说明

$$Y = X$$

即结论中的1)成立，再看(4)式变成了

$$|X| \equiv 1 \pmod{p}$$

于是结论中的2)成立。
iii) 对任意p-子群P,

$$t_{P,X} \equiv |X| \equiv 1 \pmod{p}$$

当然$t_{P,X} \neq 0$，取K是X的P不动元，(2)式意味着$P \subset K$，即结论中的3)成立。

推论51.4. （设G是有限群，$|G| = p^r m, (p, m) = 1$的p-子群，X是G的所有*Sylow* p-子群之集，则$|X||m$

证明：因G传递地作用在X上，故$|X||G| = p^r m$，另外由$|X| \equiv 1 \pmod{p}$知$(|X|, p) = 1$，故$|X||m$。
例1、72阶群一定不是单群。

证明：设G是72阶群，它的Sylow 3-子群个数为t_3，则

$$t_3 \equiv 1 \pmod{3},\ t_3|8$$

因此t_3只能是1或4。若$t_3 = 1$，则Sylow 3-子群是正规的；若$t_3 = 4$，设$X = \{K_1, K_2, K_3, K_4\}$是全体Sylow 3-子群之集。$G$作用在$X$上，即有同态$\phi : G \longrightarrow S(X) \cong S_4$。$\mathrm{Ker}(\phi)$是$G$的正规子群。只要说明$\mathrm{Ker}(\phi)$非平凡即可。首先因$|S(X)| < |G|$，故$\phi$不可能单，即$\mathrm{Ker}(\phi) \neq \{e\}$；另外若$\mathrm{Ker}(\phi) = G$，即$G$对$X$的作用是平凡的，所有元都不动，与$G$对$X$的作用传递矛盾。
例2、分类所有15阶群。设G是15阶群，记它的Sylow p-子群个数为t_p，则

$$t_3 \equiv 1 \pmod{3},\ t_3|5$$

因此$t_3 = 1$；同理$t_5 = 1$。由此可知G是循环群。可以用两种方法说明：
i) 由$t_3 = t_5 = 1$知3阶子群K_3和5阶子群K_5都是正规的，从而说明

$$G = K_3 \oplus K_5 \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/15\mathbb{Z}$$

ii) 把G中元素按阶分类：有1个1阶、2个3阶和4个5阶元；剩下8个必然是15阶元。

总结一般规律如下：若$p < q$都是素数，则pq阶群可解，此外若$q \not\equiv 1 \pmod{p}$，则pq阶群是循环群。
例3、设p, q都是素数，则p^2q阶群可解。

证明：记t_p, t_q分别为Sylow的p-子群，q-子群个数，我们断言$t_p = 1$或$t_q = 1$，即Sylow p-子群或Sylow q-子群是正规的。现设它们都非1，则由

$$t_p \equiv 1 \pmod{p},\ t_p|q$$

知$t_p = q \equiv 1 \pmod{p}$。从而$p \not\equiv 1 \pmod{q}$，故由

$$t_q \equiv 1 \pmod{q},\ t_q | p^2$$

知道$t_q = p^2 \equiv 1 \pmod{q}$，故$p \equiv -1 \pmod{q}$，结合$q \equiv 1 \pmod{p}$知道：$p = 2, q = 3$。整理所有条件如下：$G$是12阶群，它有3个4阶子群、4个3阶子群。数一数元素就会发现这不可能，因为4个3阶子群给出8个3阶元，剩下4个元，只能组成一个4阶群。

综上，我们证明了这个群是一个p^2阶群（abel）和一个q阶群的扩张，它是可解的。

练习

1、写出群S_3的所有共轭类、子群和正规子群。并回答：

(1) S_3在同构意义下有几种同态像？

(2) S_3作用在某集合X上，那么一个轨道含有的元素的数目可能是哪些值？

(3) S_3的自同态和自同构有那些？

(4) 找出S_3中满足$\sigma(12)\sigma^{-1} = (23)$的所有$\sigma$。

2、证明72阶的群一定可解。

3、代数学98页，第18、31、32题。