张劼　莫骄◎编著

JinShi DaiShu
YingYong JiChu

近世代数应用基础

北京邮电大学出版社
www.buptpress.com

近世代数应用基础

张 劼 莫 骄 编著

北京邮电大学出版社
www. buptpress. com

内 容 简 介

近世代数(又名抽象代数)是现代数学的重要基础,在信息科学、计算机科学、物理、化学等诸多学科中具有广泛应用.本书是作者在多年教学实践基础上编写的,介绍了群、环、域的基本概念、基本理论与基本应用.本书适合作为数学与应用数学、信息科学、计算机科学、物理等专业本科生、研究生教材或专业科技人员参考用书.

图书在版编目(CIP)数据

近世代数应用基础/张勐,莫骄编著.--北京:北京邮电大学出版社,2012.1

ISBN 978-7-5635-2863-9

Ⅰ.①近… Ⅱ.①张…②莫… Ⅲ.①抽象代数—高等学校—教材 Ⅳ.①O153

中国版本图书馆 CIP 数据核字(2011)第 263912 号

书　　名:近世代数应用基础

作　　者:张 勐　莫 骄

责任编辑:何芯逸

出版发行:北京邮电大学出版社

社　　址:北京市海淀区西土城路 10 号(邮编:100876)

发 行 部:电话:010-62282185　传真:010-62283578

E-mail:publish@bupt.edu.cn

经　　销:各地新华书店

印　　刷:北京联兴华印刷厂

开　　本:787 mm×960 mm　1/16

印　　张:7.25

字　　数:134 千字

印　　数:1—3 000 册

版　　次:2012 年 1 月第 1 版　2012 年 1 月第 1 次印刷

ISBN 978-7-5635-2863-9　　定　价:15.00 元

前　言

近世代数是一门非常抽象的数学学科.本书在内容编写上,力争做到抽象概念与具体实例相结合.对于群、环、域以及扩域这些基本的代数系统,我们都介绍了它们在信息工程中的具体应用.在内容顺序安排上,力争难点分散.此外,本教材还具有以下特点:

(1) 问题引入.教材以大家熟悉的问题为切入点,提高大家学习这门课的兴趣。

(2) 精炼预备知识.尽快让学生感受近世代数课程的特点,转换思维模式.

(3) 强调域上多项式,淡化一般环上多项式.降低难度,增强了实用性.

作　者

目　录

第 1 章　引言和预备知识

代数学是数学的一个古老分支，有着悠久的历史. 到 19 世纪时，代数学的研究对象和研究方法发生了巨大的变化. 人们开始关注带有运算的集合，研究方法也从以往偏重计算的思维向结构研究的思维转变，形成了所谓的近世代数学.

具有一种或几种代数运算的集合，称为代数系统. 近世代数（也称抽象代数）是研究各种抽象的代数系统的学科. 根据代数系统中的运算个数及运算所满足的性质的不同，就产生了不同的代数系统，进而形成了近世代数中各个不同的分支，其中最重要、最基本的分支是群、环和域. 目前，关于群、环、域的研究内容和方法不仅渗透到数学的各个学科，而且已经广泛应用到信息科学、计算机科学、物理、化学等诸多学科.

本课程主要介绍近世代数中最基本的代数系统——群、环和域的最基本的概念与性质.

1.1　与近世代数相关的几个问题

1.1.1　数字通信中的可靠问题

现代通信中用数字代表信息，用电子设备进行发送、传递和接收，并用计算机加以处理. 通信系统传输消息必须可靠与快速，但在数字通信系统中可靠与快速往往是一对矛盾. 若要求快速，则必然使得每个数据码元所占的时间缩短，波形变窄，能量减少，从而在受到干扰后产生错误的可能性增加，传送信息的可靠性降低. 若要求可靠，则使得传送消息的速率变慢. 如何较合理地解决可靠性与速度这一对矛盾，是正确设计一个通信系统的关键问题之一. 简单来说编码学就是在解决这对矛盾中不断发展起来的.

编码分为信源编码和信道编码. 信源编码的研究目的是提高传输效率，而信道编码

的研究目的就是提高信号传输的可靠性，纠错码是信道编码的重要研究内容. 下面用两个简单例子来说明纠错码的概念.

重复码是一个简单的纠错码，它的编码规则是一个信息元，剩下的校验元为信息元的重复. 例如，用 3 位二进制重复码表示 A，B 两个字母，A 编码为 000，B 编码为 111，则接收方收到下列信息时均译码为

接收信息：000，001，010，011，101，110，111

译码：　A，　A，　A，B，　B，　B，　B

这就意味着在译码时对其中的错误信息进行了纠正. 其中纠错的理论依据基于在信道中错 1 个比特的概率要高于 2 个比特的假设，并且译码使用了大数准则.

近世代数是进行编码设计的重要工具，较复杂的编码将在后面进行介绍.

1.1.2　数字通信中的保密问题

随着计算机科学的蓬勃发展，社会已进入信息时代. 但是电子计算机和通信网络的广泛应用，一方面为人们的生活和工作提供了便利，另一方面也提出了许多亟待解决的问题，其中信息的安全性就是一个突出的问题. 信息安全的核心技术是密码学，因此，密码学理论和技术已成为信息科学和技术中的一个重要研究领域.

密码技术主要功能是隐藏和保护需要保密的信息，使未授权者不能提取信息. 信息的原文通常称为明文，加密后的信息称为密文. 以下将借助一个古典密码来了解密码的加密解密算法.

美国电话电报公司的 Gilbert Vernam 在 1917 年为电报通信设计了一种非常方便的密码，称为 Vernam 密码. Vernam 密码在对明文加密前首先将明文编码为含有 0，1 的字符串.

设 $m=m_1m_2\cdots m_s\cdots$ 为明文，$k=k_1k_2\cdots k_s\cdots$ 为密钥，其中 m_i,k_i 取值 0 或 1($i\geqslant 1$). 则密文 $c=c_1c_2\cdots c_s\cdots$，其中

$$c_i=m_i\oplus k_i,\quad i\geqslant 1$$

这里$\oplus$为模 2 加法.

在用 Vernam 密码对明文加密时，如果对不同的明文使用不同的密钥，则这时 Vernam 密码为“一次一密”密码，而“一次一密”密码是目前被理论上证明是安全的唯一密码算法. 这种密码的安全性完全取决于密钥的随机性. 但是随机密钥的生成难以实现，并且可以看出使用这种密码无论从时间还是空间上代价都非常大. 如果不同的明文使用相同的密钥，则 Vernam 密码就比较容易破译了.

当“敌手”获取了一个密文 $c=c_1c_2\cdots c_s\cdots$ 所对应的明文 $m=m_1m_2\cdots m_s\cdots$ 时，很容易通过运算 $k_i=m_i\oplus c_i(i\geqslant 1)$ 获得密钥 $k=k_1k_2\cdots k_s\cdots$. 因此如果密钥 k 重复利用，“敌手”可以立即解密得到相应的明文.

当然，现在密码学所使用的密码算法比较复杂，算法中所涉及的运算大多数是基于代数系统的，其中基于域上的运算更多些. 因此近世代数是现代密码学最重要的数学基础. 在后续的内容上将具体介绍.

1.1.3　几何作图问题

古代数学家曾提出过几个有意思的尺(直尺)规(圆规)作图问题，规定所用的直尺没有刻度，也不能在上面作标记.

(1) 立方倍积问题：做一个立方体使其体积为一个已知立方体体积的两倍.

(2) 三等分角问题：给定任意一个角，将其三等分.

(3) 化圆为方问题：给定一个圆，做一个正方形使其面积等于已知圆的面积.

(4) 等分圆周问题：将一个圆等分成 n 份.

以上这些问题描述很简单，但直到近世代数理论出现以后才得到完全解决.

1.1.4　代数方程求根问题

方程及方程组求解是代数学研究的基本问题之一. 对于多元一次方程组的问题，我国睿智的古代数学家们早已给出了解决的办法，《九章算术》中就有专门的一章“方程”来求解此类问题. 运算采用的是被称为“遍乘直除”的方法，而这种方法实际上便是现在常用的解多元一次方程组的加减消元法.

对于一元二次方程的求根公式分别在公元 3 世纪由中国的赵爽及 600 年后的花拉子米提出. 而三次及四次方程的求根公式难住了数学家一千年，直到塔塔利亚和卡丹的出现，才发现了一般的三次和四次方程的求根公式. 18 世纪后，人们开始研究高于四次方程的代数求根的方法，但是屡战屡败. 法国数学家拉格朗日发表论文《关于代数方程解的思考》，他认为次数不低于五次的方程的代数解法一般而言是找不到的，他试图证明这个理论的正确性，但是均以失败告终. 到 19 世纪初，挪威和法国的两位天才的年轻数学家阿贝尔(Abel)和伽罗华(Galois)证明了拉格朗日的猜想，而在他们的研究工作中诞生的新概念和新理论将代数带入了一个新的时代，即抽象代数时代.

1.2 集合和映射

这一节所介绍的集合和映射的概念，在高等代数中已经学习过. 但为了和后面内容更好的衔接，在此重复一下，并统一某些标识符号.

1.2.1 集合

集合其实到目前为止，并没有统一的定义. 一般将若干个(有限或无限)固定事物的全体就叫做一个集合(简称集). 组成一个集合的事物就叫做集合的元素(简称元).

习惯用大写的英文字母表示集合，如 A,B,C 等. 元素用小写英文字母表示，比如 a，b,c 等.

若 a 是集合 A 中的元素，就说 a 属于集合 A，记为 $a\in A$. 否则就说 a 不属于集合 A，记为 $a\notin A$.

没有任何元素的集合称为空集，一般记为 $\varnothing$.

定义 1.2.1 如果集合 B 中的元素都属于集合 A，则称集合 B 是集合 A 的子集. 记为 $B\subseteq A$，或 $A\supseteq B$，读作 A 包含 B，或 B 包含于 A.

规定空集是任何集合的子集.

定义 1.2.2 如果集合 B 是集合 A 的子集，并且在集合 A 中至少存在一个元素不属于 B，则称 B 是集合 A 的真子集. 记为 $B\subset A$，或 $A\supset B$.

定义 1.2.3 如果集合 A 和集合 B 互为子集，则称两个集合相等.

定义 1.2.4 集合 A 和集合 B 的所有公共元素组成的集合，称为 A 和 B 的交集. 记为 $A\cap B$.

定义 1.2.5 由至少属于集合 A 和集合 B 之一的所有元素组成的集合称为 A 和 B 的并集. 记为 $A\cup B$.

定义 1.2.6 集合 A 和集合 B 的笛卡儿积或直积，是由 A 和 B 中所有元素构成的有序对组成的集合，记为 $A\times B$.

具体的，
$$A\times B=\{(a,b)\mid a\in A,b\in B\}$$

直积定义中的集合顺序是不能随意调换的. 例如，设 $\mathbf{Z}$ 是全体整数集，$\mathbf{Q}$ 是全体有理数集，则 $\left(2,\frac{1}{3}\right)\in\mathbf{Z}\times\mathbf{Q}$，但 $\left(2,\frac{1}{3}\right)\notin\mathbf{Q}\times\mathbf{Z}$.

上面集合的交集，并集与直积很容易推广到有限个集合上.

例 1.2.1　设 $A=\{1,2,3\}$，$B=\{-1,2\}$，则

$A\cap B=\{2\}$，$A\cup B=\{1,2,3,-1\}$，

$A\times B=\{(1,-1),(1,2),(2,-1),(2,2),(3,-1),(3,2)\}$.

1.2.2　映射

为了比较不同的集合，引入映射的概念.

定义 1.2.7　设 A,B 为两个非空集合，如果存在某个对应法则 f，使得对 A 中每一个元素 $a\in A$，都有 B 中唯一的元素 $b\in B$ 与之对应，则称 f 为集合 A 到集合 B 的一个映射，记为 $f:A\to B$.

其中 b 称为 a 在映射 f 下的象，记为 $f(a)=b$，a 称为 b 在映射 f 下的原象.

b 的所有原象组成的集合称为 b 的原象集.

若 $\forall b\in B$，都有 $a\in A$，使得 $f(a)=b$，则称映射 f 为满射.

若 $\forall a_1,a_2\in A$，当 $a_1\neq a_2$ 时，有 $f(a_1)\neq f(a_2)$，则称映射 f 为单射.

若 f 既是满射，又是单射，则称 f 为一一映射或一一对应.

特别地，设映射 $f:A\to A$，$f(a)=a$，$\forall a\in A$，称 f 为 A 的恒等映射，记为 id_A.

定义 1.2.8　如果 $\forall a\in A$，$f(a)=g(a)$，则映射 $f:A\to B$ 与 $g:A\to B$ 称为相等的.

例 1.2.2　设 $\mathbf{Z}^+$ 是全体正整数的集合，$\mathbf{R}$ 是全体实数的集合，则 $f(n)=\ln n$，$\forall n\in\mathbf{Z}^+$ 是从 $\mathbf{Z}^+$ 到 $\mathbf{R}$ 的映射. f 是单射，但不是满射.

例 1.2.3　设 $\mathbf{R}^2$ 是实平面上的全体点集，$\mathbf{R}$ 是全体实数集，则 $f(a,b)=b-a$，$\forall (a,b)\in\mathbf{R}^2$ 是从 $\mathbf{R}^2$ 到 $\mathbf{R}$ 的映射. f 是满射，但不是单射.

例 1.2.4　一元函数 $f(x)=\arcsin x$ 是从 $[-1,1]$ 到 $\left[-\frac{\pi}{2},\frac{\pi}{2}\right]$ 的一一映射.

定义 1.2.9　设有映射 $f:A\to B$，$g:B\to C$，定义映射 $gf:A\to C$ 如下：

$$(gf)(a)=g[f(a)],\forall a\in A$$

称 gf 为 g 与 f 的复合映射或 g 与 f 的乘积.

类似可定义多个映射的乘积.

映射的合成有下面的性质：

性质 1.2.1　映射的复合满足结合律.

即若有 $f:A\to B$，$g:B\to C$，$h:C\to D$，则

$$h(gf)=(hg)f.$$

证明 $\forall a\in A$，记 $f(a)=b,g(b)=c$. 则 $gf(a)=g[f(a)]=g(b)=c$，

且

$$[h(gf)](a)=h[gf(a)]=h(c);$$

又 $hg(b)=h[g(b)]=h(c)$，

所以

$$[(hg)f](a)=(hg)[f(a)]=(hg)(b)=h[g(b)]=h(c).$$

即有 $h(gf)=(hg)f$.

下面的定理给出了一一映射的充要条件.

定理 1.2.1 映射 $f:A\to B$ 为一一映射的充要条件是存在映射 $g:B\to A$，使得 $fg=id_B,gf=id_A$.

证明 充分性. 已知存在映射 $g:B\to A$，使 $fg=id_B,gf=id_A$.

$\forall b\in B$，有 $g(b)\in A$，使 $f[g(b)]=(fg)(b)=b$，故 f 为满射.

$\forall a_1,a_2\in A$，当 $a_1\neq a_2$ 时，若 $f(a_1)=f(a_2)$，则 $g[f(a_1)]=g[f(a_2)]$，由此推出 $(gf)(a_1)=a_1=(gf)(a_2)=a_2$，与 $a_1\neq a_2$ 矛盾，故 $f(a_1)\neq f(a_2)$，f 为满射.

f 既为单射又为满射，所以 f 为一一映射.

必要性. 若 f 是一一映射，下面来构造映射 $g:B\to A$，使 $fg=id_B,gf=id_A$.

$\forall b\in B$，f 是一一映射，故有唯一的 $a\in A$，使得 $f(a)=b$，规定 $g(b)=a$. 这样定义的 g 是从 B 到 A 的映射.

$\forall b\in B,(fg)(b)=f[g(b)]=f(a)=b$，即 $fg=id_B$.

又 $\forall a\in A,(gf)(a)=g[f(a)]=a,gf=id_A$.

若 f 是一一映射，称上述映射 g 为 f 的逆映射，记为 $g=f^{-1}$，由定理 1.2.1 可知 g 也是一一映射.

1.3 代数运算及运算律

定义 1.3.1 一个从集合 $A\times B$ 到集合 D 的映射 $f:A\times B\to D$ 称为一个从 $A\times B$ 到 D 的代数运算.

一般用$\circ$表示这个运算，即 $\forall (a,b)\in A\times B$，将 $f((a,b))$ 记为 $a\circ b$.

若$\circ$是从 $A\times A$ 到 A 的代数运算，即 $\forall a,b\in A,a\circ b\in A$，则称$\circ$是 A 的代数运算或称$\circ$是 A 的二元运算. 当然 A 对于运算$\circ$是封闭的.

例 1.3.1　设 A_1 为所有 2×3 阶实矩阵构成的集合，A_2 为所有 3×2 阶实矩阵构成的集合，A_3 为所有 2 阶实矩阵构成的集合. $\forall A\in A_1$，$\forall B\in A_2$，

$$A\circ B\overset{定义}{=}AB(\text{矩阵乘积}),$$

则$\circ$为 $A_1\times A_2$ 到 A_3 的代数运算，这个运算就是矩阵的乘法.

例 1.3.2　设 $\mathbf{R}$ 为全体实数集，$A=\{\ln x\mid x>0,x\in\mathbf{R}\}$. $\forall \ln a,\ln b\in A$，定义

$$\ln a\circ\ln b=\ln ab(=\ln a+\ln b),$$

则$\circ$是 A 的代数运算，这个运算就是普通数的加法.

定义 1.3.2　称一个 $A\times A$ 到 A 的代数运算$\circ$满足结合律，如果 $\forall a,b,c\in A$，有

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

如果 A 的代数运算$\circ$适合结合律，用数学归纳法可以证明，对 A 的任意 n 个元素 a_1，a_2，$\cdots$，a_n 来说，所有的 $\pi(a_1\circ a_2\circ\cdots\circ a_n)$ 都相等，我们用 $a_1\circ a_2\circ\cdots\circ a_n$ 来表示这个唯一的结果. 其中 $\pi(a_1\circ a_2\circ\cdots\circ a_n)$ 表示对 $a_1\circ a_2\circ\cdots\circ a_n$ 用某种两两加括号的步骤运算后所得到的结果.

例如，$a_1\circ a_2\circ a_3=(a_1\circ a_2)\circ a_3=a_1\circ(a_2\circ a_3)$；

$a_1\circ a_2\circ a_3\circ a_4=(a_1\circ a_2)\circ a_3\circ a_4=a_1\circ(a_2\circ a_3)\circ a_4=a_1\circ a_2\circ(a_3\circ a_4)$.

定义 1.3.3　称一个 $A\times A$ 到 D 的代数运算$\circ$满足交换律，如果 $\forall a,b\in A$，有

$$a\circ b=b\circ a.$$

同样，用数学归纳法可以证明，当 A 的代数运算$\circ$同时适合结合律与交换律时，$a_1\circ a_2\circ\cdots\circ a_n$ 中元素的次序可以调换.

结合律和交换律描述的是一种代数运算的性质. 两种代数运算之间的性质用分配律描述.

设$\odot$是 $B\times A$ 到 A 的代数运算，$\oplus$是 A 的代数运算. $\forall b\in B$，$\forall a_1,a_2\in A$，$b\odot(a_1\oplus a_2)$，$(b\odot a_1)\oplus(b\odot a_2)$ 都有意义，且都是 A 中的元素，但它们不一定相等.

定义 1.3.4　设$\odot$是 $B\times A$ 到 A 的代数运算，$\oplus$是 A 的代数运算，称代数运算$\odot$，$\oplus$满足右分配律，如果 $\forall b\in B$，$\forall a_1,a_2\in A$，有

$$b\odot(a_1\oplus a_2)=(b\odot a_1)\oplus(b\odot a_2).$$

例如，假设 B 和 A 都是全体实数的集合，$\odot$和$\oplus$是普通的乘法和加法，上式就变成了

$$b(a_1+a_2)=(ba_1)+(ba_2).$$

定义 1.3.5　设$\odot$是 $A\times B$ 到 A 的代数运算，$\oplus$是 A 的代数运算，称代数运算$\odot$，$\oplus$满足左分配律，如果 $\forall b\in B$，$\forall a_1,a_2\in A$，有

$$(a_1\oplus a_2)\odot b=(a_1\odot b)\oplus(a_2\odot b).$$

用数学归纳法可以证得，如果$\oplus$满足结合律，且$\odot$和$\oplus$满足右分配律，那么$\forall b\in B$，$\forall a_1,a_2,\cdots,a_n\in A$，有

$$b\odot(a_1\oplus a_2\oplus\cdots\oplus a_n)=(b\odot a_1)\oplus(b\odot a_2)\oplus\cdots\oplus(b\odot a_n).$$

同样，如果$\odot$和$\oplus$满足左分配律，就有

$$(a_1\oplus a_2\oplus\cdots\oplus a_n)\odot b=(a_1\odot b)\oplus(a_2\odot b)\oplus\cdots\oplus(a_n\odot b).$$

分配律的重要性在于它刻画了两种代数运算的联系，使两种运算融合到一起.

1.4 等价关系与集合的分划

定义 1.4.1 设A是集合，集合$A\times A$的每个子集R称为集合A上的一个(二元)关系. 若$(a,b)\in R$，则称a和b有关系R，写成aRb.

例 1.4.1 设$\mathbf{R}$为全体实数集，$\mathbf{R}\times\mathbf{R}$中的子集$R=\{(a,b)\in\mathbf{R}\times\mathbf{R}\mid a>b\}$就是$\mathbf{R}$上的一个关系，$aRb$指的是$a>b$.

例 1.4.2 设$\mathbf{Z}$为全体整数集，$\mathbf{Z}\times\mathbf{Z}$中的子集$R=\{(a,b)\in\mathbf{Z}\times\mathbf{Z}\mid 3\text{ 整除 }(a-b)\}$就是$\mathbf{Z}$上的一个关系. mRn指的是$m-n=3k,k\in\mathbf{Z}$，即m与n模3同余，记为$m\equiv n(\mathrm{mod}\ 3)$.

本课程关心的是等价关系，定义如下：

定义 1.4.2 集合A的一个二元关系R称为等价关系，如果它满足以下三条性质：

(1) 反身性：$\forall a\in A,aRa$；

(2) 对称性：$\forall a,b\in A$，若aRb，则bRa；

(3) 传递性：$\forall a,b,c\in A$，若aRb,bRc，则aRc.

若R是等价关系，则aRb记为$a\sim b$. 例1.4.2中的二元关系是等价关系，例1.4.1中的二元关系就不是等价关系.

定义 1.4.3 若把集合A分成若干个子集，使得A中的每一个元素属于且只属于一个子集，则称这些子集的全体为集合A的一个分划. 每个子集称为A的一个类.

等价关系与集合的分划是一一对应的.

定理 1.4.1 集合A的一个分划决定A的一个等价关系.

证明 给定A的一个分划后，集合A被分成若干个类的并，A中的每一个元素属于且只属于一个类.

令$R=\{(a,b)\in A\times A\mid a$与$b$在同一类$\}$，下面证明$R$是$A$上的一个等价关系.

第一，$\forall a\in A$，因为$(a,a)\in A\times A$，且 a 与 a 在同一类，所以$(a,a)\in R$，即 aRa，这说明 R 具有反身性；第二，$\forall a,b\in A$，如果 aRb，即$(a,b)\in R$，则 a 与 b 在同一类，于是$(b,a)\in R$，即 bRa，这说明 R 具有对称性；第三，$\forall a,b,c\in A$，如果 aRb,bRc，即$(a,b)\in R,(b,c)\in R$，因此 a 与 b 在同一类，b 与 c 在同一类，所以 a 与 c 在同一类，故$(a,c)\in R$，即 aRc，这说明 R 具有传递性.

定理 1.4.2　集合 A 的一个等价关系～决定 A 的一个分划.

证明　记$[a]=\{b\in A\mid b\sim a\}$，即$[a]$是所有与 a 等价的元素全体，称为 a 所在的等价类，a 是代表元.

下面证明 $A=\bigcup\limits_{a\in A}[a]$是 A 的一个分划. 先说明等价类与代表元无关，即若 $a\sim b$，则 $[a]=[b]$.

事实上，若 $c\in[a]$，则 $c\sim a$，又 $a\sim b$，由等价关系的传递性可知 $c\sim b$，所以 $c\in[b]$，故 $[a]\subseteq[b]$.

类似可证明$[b]\subseteq[a]$，因此$[a]=[b]$.

再来说明 A 中任意元必属于且仅属于某一个类. $\forall a\in A$，易知 $a\in[a]$；若 $a\in[b]$且 $a\in[c]$，则 $b\sim a,a\sim c$，于是 $b\sim c$，$[b]=[c]$.

定义 1.4.4　设集合 A 有一个分划，每类中的任意元素称为该类的一个代表. 刚好由每一类的一个代表所构成的集合叫做 A 的完全代表系.

如例 1.4.2 中的等价关系确定了 $\mathbf{Z}$ 的一个分划，在这个分划下 $\mathbf{Z}$ 的完全代表系为 $\{0,1,2\}$.

其中$[0]=\{3k\mid k\in\mathbf{Z}\}$；$[1]=\{3k+1\mid k\in\mathbf{Z}\}$；$[2]=\{3k+2\mid k\in\mathbf{Z}\}$.

$[0],[1],[2]$称为模 3 的剩余类.

最后介绍本节的另一个重要概念.

定义 1.4.5　设集合 A 中有代数运算$\circ$，若 A 的一个等价关系～满足

$$\forall a,b,c,d\in A,a\sim b,c\sim d\Rightarrow a\circ c\sim b\circ d,$$

则称～为$\circ$的一个同余关系. $a\in A$ 所在的等价类$[a]$称为 a 的同余类.

例 1.4.3　设 m 为正整数，$\mathbf{Z}$ 为全体整数的集合，在 $\mathbf{Z}$ 中定义关系～：

$$a\sim b\Leftrightarrow a\equiv b(\mathrm{mod}\ m).$$

易证～是等价关系. 且由 $a\equiv b(\mathrm{mod}\ m)$，$c\equiv d(\mathrm{mod}\ m)$，可得

$$a+c\equiv b+d(\mathrm{mod}\ m),ac\equiv bd(\mathrm{mod}\ m).$$

因此～对于 $\mathbf{Z}$ 中的加法和乘法都是同余关系.