群

2023 年 5 月 25 日

目录

这一章我们主要来论述群论，群论是伽罗瓦在他那个时代为了要解决的几个首要的数学问题而创造的，那个问题是：什么时候可以用二次公式的某个推广找到一个多项式的根？而关于之前的证明，运用群论也可以得到一些漂亮的证明，例如费马定理，也适合用来解决计数问题。

1　一些集合理论

一个群是一个集合，其元素可以被“乘”，且乘法遵循一定的法则，群的重要例子是其元素为置换且置换是某些函数，然后我们将用函数把两个群做比较，称为同态，所以我们接下来主要讲一些定义：和函数的基本性质。

集合X是指一些特定事物组成的一个整体，例如点，马，人类等等，若x是X的元素，就说x属于X，记为 $x \in X$，若两个集合X, Y是相等的，记作

$$X = Y$$

如果它们都由完全相同的元素组成，即对任何的元素x，存在$x \in X$当且仅当$x \in Y$

集合S称为集合X的子集，是指S的元素都属于X，即$s \in S$且$s \in X$，我们记为

$$S \subseteq X$$

且S是X的子集，我们也叫做S包含于X，若$S \subseteq X$且$S \neq X$，那么我们把S叫X的真子集，记为$S \subsetneq X$，如果$S \subseteq X$，且$S \neq X$。两个集合X, Y相等当且仅当每个集合是另一个集合的子集。即

$$X = Y \text{当且仅当} \quad X \subseteq Y \text{且} Y \subseteq X$$

所以，当我们想证明两个集合相等的时候，只需要证明两个部分，即两个集合是否是互相包含，也就是证明一个集合是另一个的子集。例如，我们令

$$X = \{a \in R | a \geq 0\},\ Y = \{b \in R | b = r^2, r \in R\}$$

我们设$a \in X$，则$a \geq 0$ ，且$a = r^2$，那么$r = \sqrt{a}$，所以$a \in Y$，这样子$X \subseteq Y$，反过来，我们取$b \in Y$，使得对某个$r \in R$存在$b = r^2 \in Y$，且$r \geq 0$的时候$r^2 \geq 0$，当$r < 0$的时候同样的$r^2 > 0$，所以$b \in X$有$Y \subseteq X$，为此$X = Y$

交、并集

空集是指不含任何元素的集合$\emptyset$

1.1 定义：交集

若X, Y是Z的子集，则它们的交是集合

$$X \cap Y = \{z \in Z; z \in X \text{且 } z \in Y\}$$

更一般的，我们定义：若$\{A_i, i \in I\}$是集合Z的一族子集，其中I是指标集，且集合个数可能无穷多个，则我们定义：交为

$$\bigcap_{i\in I} A_i = \{z \in Z, z \in A \text{对所有} i \in I \text{成立}\}$$

1.2 定义：并集

若X, Y是Z的子集，则定义：并为

$$X \cup Y = \{z \in Z; z \in X \text{或者} z \in Y\}\}$$

更一般的，若$\{A_i; i \in I\}$是Z任意的一族子集，可能无穷多个，我们构造并为

$$\bigcup_{i\in I} = \{z \in Z; z \in A_i \text{对某个} i \in I \text{成立}\}$$

对于交集，显然交集是两个集合中共同的元素，即$X \cap Y \subseteq X$，$X \cap Y \subseteq Y$，反过来，若$S \subseteq X$和$S \subseteq Y$，那么$S = X \cap Y$

而对于并集，就是把所有的元素合在一起。显然有$X \subseteq X \cup Y$和$Y \subseteq X \cup Y$，若$X \subseteq S$且$Y \subseteq S$，则$X \cup Y \subseteq S$

1.3 差集

若X, Y是集合，则它们的差是集合

$$X - Y = \{x \in X; x \notin Y\}$$

差集表示，$X - Y$中X不含有Y的元素，反过来，$Y - X$则表明Y中不包含X的元素。显然，利用差集，我们可以定义：补集，若X是集合Z的一

个子集，则X在Z中的补集我们定义：为

$$X' = Z - X = \{z \in Z; z \notin X\}$$

显然X'与X是不相交的，所以$X \cap X' = \emptyset$。

2 函数

函数指的是一种特殊的法则，例如常见的$x^2, e^x, ln(x)$等都是常用的函数，在之前的书，我们定义：函数$f(x)$为一个法则，法则要求对于每个a，恰好分配一个数与$f(a)$对应，因此，平方函数把81分配给9，平方根函数则把3分配给9

一个显著的问题是，既然我们已经定义：了函数，什么时候两个函数相同，例如考虑函数

$$f(x) = (x+1)^2,\ \ g(x) = x^2 + 2x + 1$$

$f(x) = g(x)$成立吗，因为它们的计算过程不同，考虑$x = 3$有$f(3) = 4^2$，而$g(3) = 3^2 + 2 \times 3 + 1$，因为我们并没有清楚的定义：法则，所以含义是模糊的，我们也不能回答问题。为了找到一个合理的定义：，我们重新回到函数定义：的例子上，函数$x^2, \sin x$都有一个形如$(a, f(a))$的点构成一个平面上的图形，是平面的子集，例如$f(x) = x^2$图形就是形如(a, a^2)所构成的抛物线。

图形是直观的，我们接下来要讲的关于函数的正式定义：也相当于是要描述函数具有自己的图形，首先我们得给出类似平面的概念。

2.1 笛卡尔积

若X, Y都是集合（不一定不相同），则称对所有有序对$(x.y)$组成的集合$X \times Y$称为它们的笛卡尔积，其中$x \in X,\ y \in Y$

一个常见的例子是平面，我们记为$R \times R$或者R^2前者表示是两个直线的笛卡尔积构成的一个特殊集合，后者则是表示“二维”，另一个例子是：$X = \{1, 2, 3\},\ \ Y = \{4, 5, 6\}$，那么它的笛卡尔积是

$$X \times Y = \{(1,4),(1,5),(1,6),(2,4),(2,5).(2,6),(3,4),(3,5),(3,6)\}$$

而对于有序对，我们只需要知道，当

$$(x, y) = (x', y') \quad \text{当且仅当} \quad x = x', y = y'$$

若X, Y都是有限集，我们不妨设$|X| = m$，$|Y| = n$，其中$|X|$表示集合含有的元素个数，那么$|X \times Y| = mn$。利用刚才的例子，很好理解，每个X的元素对应着每个Y中的元素，利用排列的知识，每个$x \in X$有3种可能，而$|X| = 3$所以就是3×3种可能，所以$|X \times Y|$一共有9个元素。

2.2　定义：函数

设X, Y都是集合，子集$f \subseteq X \times Y$，若对每个$a \in X$，则存在唯一的$b \in Y$使得$(a, b) \in f$，则称f为X到Y的一个函数，记为

$$f : X \to Y$$

对每个$a \in X$，我们称满足$(a, b) \in f$的唯一元素$b \in Y$为f在a处的值，并记为b为$f(a)$，因此，f是由$X \times Y$中所有形如$(a, f(a))$的点构成的，为此，当$f : R \to R$的时候，f是$f(x)$的图像。

2.2.1 一些函数的例子

1. 恒等函数：我们设X是一个集合，我们说集合X上的恒等函数，记为$1_X : X \to X$，定义对每个$x \in X$都有$1_X(x) = x$，当$X = R$的时候，图形就像是一个由(a, a)的点组成的$45°$的直线。

2. 常数函数：若$y_0 \in Y$，则对所有的$x \in X$都有$f(x) = y_0$(当$X = R = Y$的时候，常数函数的图形是水平直线)

为了简便，我们使用f表示一个函数，而不是$f(x)$，当我们要表示一个具体的函数值的时候我们才会使用$f(x)$。但我们将继续使用通常的记号表示一些熟悉的函数，例如$\sin x, e^x, \cdots$多项式等等。若$f : X \to Y$，我们把X叫做定义域，把Y叫目标域（或者上域），并定义f的值域（或范围）为$\mathbf{im} f$，它是由所有f的值构成的Y的子集。

当我们说X是函数$f : X \to Y$的定义域时，意思是$f(x)$对每个$x \in X$都存在定义，例如$\sin x$的定义域是R，目标域通常为R，但值域是$[-1, 1]$，这很好理解，因为对于一个$\sin x$，它的一个一般化的函数（经过我的简化，我把全部东西丢到x里了）是$A \sin(x)$，其中A是任意常数，为此藉由这个函数我们可以把一般的$\sin x$推广到任意大的目标域上。对于另一个函数$1/x$，它的定义域是所有非负实数构成的集合，值域也是非零实数集合。用集合的语言描述就是$1/x$的定义域的集合为：$X = \{x \in R \mid x \neq 0\}$，而平方根函数的定义域是所有非负实数构成的集合$R^{\geq} = \{x \in R : x \geq 0\}$，且值域也是$R^{\geq}$

2.2.2 函数相等

我们说两个函数$f : X \to Y$和$g : X' \to Y'$相等，若$X = X'$, $Y = Y'$，且子集$f \subseteq X \times Y$和$g \subseteq X' \times Y'$相等

这意味着我们判断函数需要看三个重要的组成部分，当我们定义$f : X \to Y$的时候，我们定义了定义域X，目标域Y和图像，当我们说两个函数相等的时候当且仅当它们存在相同的定义域，且有相同的目标域和图像。这意味着若函数相同则两者的图像是重合的。

2.2.3 定义：对函数的限制

若$f: X \to Y$是一个函数，S是X的一个子集，则f对S的限制是函数$f \mid S: S \to Y$，定义为对所有的$s \in S$有$(f \mid S)(s) = f(s)$

这意味着对函数的限制取的是定义域上的一部分做运算。若S是X的一个子集，则定义包含$i: S \to X$为如下函数，对所有的$s \in S$有$i(s) = s$

若S是X的一个真子集，则包含i不是恒等函数1_S，因为目标域是X而不是S，但也不是恒等函数1_X，因为定义域是S而不是X，若S是X的一个真子集，则$f \mid S \neq f$，因为定义域不同

2.2.4 命题

设$f: X \to Y$, $g: X \to Y$都是函数，而$f = g$当且仅当$X = X'$, $Y = Y'$且对每个$a \in X$存在$f(a) = g(a)$

这个命题就很好的解决了函数相等的问题，例如刚才给出的$f(x) = (x+1)^2$和$f(x) = x^2 + 2x + 1$是否相等的问题。

证明： 假设$f = g$，因为函数都是$X \times Y$的子集，那么$f = g$的意思是f, g中的每个都是另一个的子集（或者通俗来说有相同的图形），若$a \in X$且$(a, f(a)) \in f = g$,则$(a, f(a)) \in g$，但g中只存在一个有序对与a对应，即$(a, g(a))$，那么只有一种可能$(a, f(a)) = (a, g(a))$，再利用有序对的相等可知，$f(a) = g(a)$，为此$f = g$

反之，我们假设对每个$a \in X$有$f(a) = g(a)$，为了证明$f = g$，我们必须要证明$f \subseteq g$和$g \subseteq f$，f的元素具备形式$(a, f(a))$，由于$f(a) = g(a)$，那么有序对$(a, f(a)) = (a, g(a))$，那么$(a, f(a)) \in g$，所以$f \subseteq g$，对于另一种包含关系，我们有$a \in X$，$(a, g(a)) = (a, f(a))$，那么就有$(a, g(a)) \in f$，则$g \subseteq f$。那么由于f, g互相包含，这意味着$f = g$

那么在刚才的证明我们看到，若函数$f, g: X \to Y$取不同的值，甚至只在一点取不同的值，即存在一个$a \in X$使得$f(a) \neq g(a)$，那么$f \neq g$

我们继续把函数看作是$x \in X$映到$f(x) \in Y$的一个法则，但为了方便我们只是单纯的这样子记，如果有必要，我们才进行精确的定义，就像刚才举得例子一样。然而，我们只是强调$f: X \to Y$把X的点映到Y中这点动态行为，所以我们一般用

$$f: x \to y$$

而不是$f(x)=y$，例如，我们可以写$f:x\to x^2$而不写$f(x)=x^2$。而且可以用$f:x\to x$描述恒等映射。

例子

我们考虑一个退化的例子，设X是一个集合，那么函数$X\to\emptyset$是什么样子的。注意的是，$X\times\emptyset$是不存在的的，因为不存在$y\in\emptyset$，这意味着不存在有序对$(x,y)\in X\times\emptyset$。所以$X\times\emptyset=\emptyset$，函数$X\to\emptyset$是某个类型的$X\times\emptyset$的子集。但$X\times\emptyset$是空集，只存在一个子集也就是空集，为此只有一个函数能到达目的地，即$f=\emptyset$，但函数$X\to\emptyset$的定义要求对每个$x\in X$都存在唯一的元素$y\in\emptyset$满足$(x,y)\in f$，当$X\neq\emptyset$时，存在$x\in X$但不存在这样子的y，所以f不是一个函数，所以$f=\emptyset$是$\emptyset\to\emptyset$这只能说明它就是恒等函数$1_\emptyset$

我们之前描述，关于值域和上域的区别，值域$\mathrm{im}f$指的是我们可以得到关于函数的实际值，但上域是包含实际值的。那么我们藉由拓展一些定义

2.3 满射

我们称函数$f:X\to Y$是满射(或到点上)，若$\mathrm{im}f=Y$

所以，若对$y\in Y$存在某个$x\in X$（可能依赖Y）使得 $y=f(x)$，则f是满射。

例子2

1. 恒等函数是满射：
2. 正弦函数$R \to R$不是满射，因为目标域是R，但$\mathrm{im} f$是$[-1,1]$，其中$\mathrm{im} f \subseteq R$
3. 函数$x^2 : R \to R$和$e^x : R \to R$都不是满射，因为前者$\mathrm{im} x^2$是非负实数，后者一样 e^x的值也是非负实数，因为$e^{-1} = 1/e > 0$。
4. 设$f : R \to R$，为了搞清楚f是否是满射，我们要问是否每个$b \in R$都有形式$b = f(a)$，即给定b，我们能否求出a使得

   $$6a + 4 = b?$$

   我们总可以解这个关于a的方程得到$a = \frac{1}{6}(b-4)$，所以f是一个满射。
5. 看下面的这个方程，设$f : R - \{\frac{3}{2}\} \to R$，即在$(-\infty, 3/2) \cup (3/2, \infty)$上定义有函数

   $$f(a) = \frac{6a+4}{2a-3}$$

   为了弄清f是否是满射，给定b去求解a，那么方程为 $a(6-2b) = -3b-4$，若$6-2b \neq 0$，则可以解出a。而且注意，定义不包含$(-3b-4)/(b-2b) \neq 3/2$。所以，方程也暗示了当$b = 3$的时候是没有解的。因为当$b = 3$的时候分母为0，是错误的。且，当$(6a+4)/(2a-3) = 3$，交叉相乘会得到$6a+4 = 6a-9$是错误的方程。所以$3 \notin \mathrm{im} f$，f不是满射

有时候我们并不能说一个函数f的值是唯一的，改说f是单值的，例如，若$R^{\geq}$表示非负实数，则$\sqrt{} : R^{\geq} \to R^{\geq}$，因为对于一个正数，开根号得到的结果是正的是显然的，但另一方面，$f(a) = \pm\sqrt{a}$不是单值的，所以由命题不是函数。（因为我们一开始已经说函数是一一对应的了）

那么藉由这个例子我们定义真正的函数

2.4 定义：单射

我们称函数$f : X \to Y$是单射的（一对一），若只要a, a'是不同的元素，则$f(a) \neq f(a')$，也就是说当f是单射，若对$a, a' \in X$，有$f(a) = f(a') \Rightarrow a = a'$

但，单值和单射的描述是颠倒的，单值指的是对于两个不同的值a, a'，有$f(a) = f(a')$，而单射指的是对于两个值的映射是一样的有两个值是相等的，即$f(a) = f(a') \Rightarrow a = a'$。

例3

我们依然使用例2的5，我们设$f : R - \{\frac{3}{2}\} \to R$由下式定义

$$f(a) = \frac{6a+4}{2a-3}$$

为了检验是否是单射，我们假设$f(a) = f(b)$，这意味

$$\frac{6a+4}{2a-3} = \frac{6b+4}{2b-3}$$

现在交叉相乘有

$$12ab + 8b - 18a - 12 = 12ab + 8a - 18b - 12$$

这表明$26a = 26b$，所以$a = b$，所以f是单射。但在之前的分析我们知道它不是满射。

2.5 定义：复合函数

若$f : X \to Y$，且$g : X \to Y$，那么它们的合成，记为$f \circ g$，被定义为下式给定的函数$X \to Z$

$$g \circ f : x \to g(f(x))$$

定义表明了，复合函数是把一个函数当成变量传入另一个函数中，所以这种合成有两个步骤，先$x \to f(x) \to g(f(x))$，例如给出函数$h : R \to R$，$h(x) = e^{\cos x}$就是合成的函数，其中$f(x) = \cos x$且$g(x) = e^x$当我们若要计算$h(\pi)$的时候，先计算$f(\pi) = cos(\pi) - 1$然后带入$g(-1) = e^{-1} = e^{-1}$

注意的是$f \circ g \neq g \circ f$，考虑$f : n \to n^2$和$g : n \to 3n$，而$g \circ f : 2 \to$

$g(4)=12$，但$f\circ g:2\to f(6)=36$。虽然不满足交换律，但满足结合律

2.6 引理

函数的合成满足结合律：若

$$f:X\to Y,\ g:Y\to Z\text{和}h:Z\to W$$

都是函数，则

$$h\circ(g\circ f)=(h\circ g)\circ f$$

证明: 我们必须证明两个合成元素$a\in X$的值都是$w=h(g(f(a)))$，若$x\in X$，则

$$h\circ(g\circ f):x\to(g\circ f)(x)=g(f(x))\to h(g(f(x)))=w$$

和

$$(h\circ g)\circ f:x\to(h\circ g)(f(x))\to h(g(f(x)))=w$$

所以满足结合律。

2.7 引理

设$f:X\to Y$，则$1_Y\circ f=f=f\circ 1_X$

证明：我们设$x\in X$则

$$1_Y\circ f:x\to 1_Y(f(x))\to f(x)$$

和

$$f\circ 1_X:x\to x\to f(x)$$

成立。上述例子给了我们一个提示，是否存在$F(x)$的倒数，这是说，对于函数f，是否有$g\in F(x)$使得$f\circ g=1_X$，或者$g\circ f=1_X$

为了回答这个问题，我们先讨论一些其他的

2.8 定义：双射

函数$f:X\to Y$称为双射的，如果它即为单射又为满射。

例4

1. 恒等函数总是双射的

2. 设$X=\{1,2,3\}$，定义$f:X\to X$为

$$f(1)=2,f(2)=3,f(3)=1$$

明显函数是双射。

利用例4的2，我们可以来研究函数的逆运算。

2.9 定义：反函数

函数$f:X\to Y$有反函数（或逆），如果存在函数$g:Y\to X$使得$g\circ f$和$f\circ g$都是恒等函数。

逆是自然的定义，例如$f=2x:R\to R$和$g=1/2x:R\to R$，则$f\circ g=2(1/2x)=x$是成立的，所以g是f的反函数。但这有个比较特殊的性质，现在我们来描述

2.10 引理

若$f:X\to Y$和$g:Y\to X$满足$g\circ f=1_X$，则f是单射且g是满射。

证明：假设$f(a)=f(a')$，则$g(f(a))=g(f(a'))$，因为$g(f(a))=a$，那么$a=a'$。所以f是单射。设$x\in X$，那么$x=g(f(x))$，这样子$x\in \mathrm{img}$，所以g是满射。

满足单射和满射说明对于每个$y\in Y$，都存在唯一的x对应，这表明$X\times Y$的每个元素都是独一无二的,不存在任意的$a,a'\in X$和$f(a)$，$f(a')\in Y$使得$(a,f(a))=(a',f(a'))$。所以我们给出命题

2.11 命题

函数$f:X\to Y$有反函数$g:Y\to X$当且仅当f是双射。

证明：若f存在反函数g，则由引理2.11表示f是单射也是满射，因为$g\circ f$和$f\circ g$都是恒等函数。

我们假设f是双射，那么$y\in Y$，由于f是满射，就存在某个$a\in X$使得$f(a)=y$，且f是单射，所以a是唯一确定的。我们定义$g(y)=a$，则g是一个单值函数，定义域是Y。显然g就是f的一个反函数。那么就对所有的$y\in Y$有$f(g(y))=f(a)=y$，且对所有的$a\in X$ 有$g(f(a))=g(y)=a$

双射f的反函数记为f^{-1}，并且一个函数不可能具备两个反函数，这与我们的命题2.11冲突，并且在三角函数中对反三角函数我们也是这么干的例如$\sin^{-1} x = \arcsin x$且满足$\sin(\arcsin x) = x$。而且，$\sin^{-1} x$不是指$1/\sin x$，$1/\sin x = \csc x$

例4

我们可以找到两个函数f, g满足$g \circ f$是恒等函数，但$f \circ g$不是恒等函数，所以f, g不互为反函数。
定义$f, g : N \to N$如下

$$f(n) = \quad n+1$$
$$g(n) = \begin{cases} 0 & n = 0 \\ n-1 & n \geq 1 \end{cases}$$

那么$g \circ f = 1_N$，因为$g(f(n)) = g(n+1) = n$（其中$n+1 \geq 1$），另一方面$f \circ g \neq 1_N$，因为$f(g(0)) = f(0) = 1 \neq 0$。

2.12 命题

若集合X到自身的所有双射构成的集合记为S_X，则函数的合成满足以下性质

1. 若$f, g \in S_X$，则$f \circ g \in S_X$
2. 对所有的f, g，$h \in S_X$，$h \circ (g \circ f) = (h \circ g) \circ f$
3. 恒等函数1_X位于S_X中，且对每个$f \in S_X$有$1_X \circ f = f \circ 1_X = f$
4. 对每个$f \in S_X$存在$g \in S_X$满足$g \circ f = 1_X = f \circ g$

2.13 定义：集合相等

两个集合（可能是无限集）X, Y有相同的元素个数，记为$|X| = |Y|$，若存在一个双射$f : X \to Y$

如果集合X称为可数的，若X是有限集或者与自然数集N有相同的元素个数。这意味着给定一个双射$f : N \to X$，都能把X的元素不重复的列出

来。但也有不可数的集合，例如R就是不可数的，这个证明由康托尔给出。这意味着R是不可数的，如果一个数z是代数数，这说明z可以表示为某个多项式$f(x)=q_0+q_1x+\cdots+q_nx^n$的根。其中$q_0,\cdots,q_n$都是有理数。如果$z$是超越数，则说明不是代数数，但有理数$r$全都是代数数，因为$x-r$是其的一个根，但无理数也存在代数数，例如$\sqrt{2}$是$x^2-2$的根。但代数数只可能是可数个的，再由康托尔的不可数性可知，超越数是不可数个的。

3 等价关系

我们来定义一个比较重要的概念-等价关系

3.1 定义：关系

给定集合X,Y，X到Y的一个关系指的是$X\times Y$的一个子集R，若$X=Y$，则我们说R是X上的一个关系，我们一般写为xRy，而不是$(x,y)\in R$

我们给出一个例子

定义关系$R=\{(x,y)\in R\times R\mid (x,y)$在y=x上或者上方$\}$。我们来验证$x\leq y$当且仅当$(x,y)\in R$，$R$定义为$(x,y)$在$y=x$的上方或者在直线上，当$x=1$的时候，$y\geq 1$，当$x=2,y\geq 2$满足要求，而$x=1,y=0.5$或者任意$y\leq 1$的情况都不是$R$中的元素，所以$x\leq y$当且仅当$(x,y)\in R$

例5

1. 每个函数$f:X\to Y$是X到Y的一个关系
2. 相等是任何集合X上的一个关系
3. $\bmod m$同余是Z上的一个关系

3.2 定义：关系$x \equiv y$

自反的：对所有$x \in X$有$x \equiv x$

对称的：对所有的$x, y \in X$若$x \equiv y$，则$y \equiv x$

传递的：对所有的$x, y, z \in X$，若$x \equiv y$和$y \equiv x$，则$x \equiv z$

若X上的一个关系满足三条性质：自反性、对称性、传递性，则说该关系是X上的一个等价关系

例6

1 普通的相等关系是任意集合上的一个等价关系

2 若$m \geq 0$，则说明上述同余的三个性质有$x \equiv y \mod m$是$X = Z$上的一个等价关系

3 设$X = \{(a, b) \in Z \times Z \mid b \neq 0\}$，并定义$X$上的一个关系$\equiv$为交叉相乘

$$(a, b) \equiv (c, d) \quad 当 \quad ad = bc$$

我们断言其是一个等价关系，其中自反性和对称性的验证比较容易，$(a, a) = (c, c)$有$ac = ca$成立$(b, a) \equiv (d, c)$有$bc = ad \Rightarrow ad = bc$，对于传递性，我们假设$(a, b) \equiv (c, d)$和$(c, d) \equiv (e, f)$，那么由于$ad = bc$，就有$adf = bcf$，而且因为$cf = de$就有$bcf = bde$,这表明$adf = bde \Rightarrow af = be \Rightarrow (a, b) \equiv (e, f)$

3.3 定义：等价类

设$\equiv$是集合X上的一个等价关系，若$a \in X$，则a的等价类记为$[a]$，定义为

$$[a] = \{x \in X \mid x \equiv a\} \subseteq X$$

那么我们应该可以找出一些等价类，注意到若$x \equiv y$则满足自反、对称、传递的性质那么给出一些例子。

例7

1 我们设$\equiv$是集合X上的相等关系，若$a \in X$，那么a只能含有一个元素，等价类就是$[a] = \{a\}$，因为$x = a$，只能是两个数相等。

2 我们现在考虑Z上的模m同余，模运算是等价的关系，这是一定的。所以，为了解决找出同余类的事情，我们需要用到同余的东西。我们总能对$ax \equiv y(\mod m)$（(a,m)=1）总是有解的。也就是说一个同余类定义是

$$\{x \in Z \mid x = a + km,\ k \in Z\} \tag{1}$$

$$\{x \in Z \mid x \equiv a \mod m\} \tag{2}$$

其中1是2 的解形式，所以这意味着对于$x \equiv a \mod m$当且仅当对某个$k \in Z$有$x = a + km$，这两个子集是一致的，即等价类$[a]$是全部的同余类

3.4 引理

若$\equiv$是集合X上的一个等价关系，则$x \equiv y$ ，则$x \equiv y$当且仅当$[x] = [y]$

证明： 我们假设$x \equiv y$，若$z \in [x]$，则$z \equiv x$，有传递性可知$z \equiv y$，所以$[x] \subseteq [y]$，然后根据对称性有$y \equiv z$，那么有$[y] \subseteq [x]$，所以$[x] = [y]$

反之，若$[x] = [y]$，根据自反性就有$x \in [x]$有$x \in [x] = [y]$有$x \equiv y$

这个引理告诉我们，在等价类替代元素的条件下，我们可以使用相等代替等价。

3.5 定义：集合的分类

集合X的一族子集P称为两两不相交，若对所有$A, B \in P$都有$A = B$或者$A \cap B = \emptyset$。而集合X的一个分类指的是，一族两两不相交的子集（称为块）并且它们的并是 X

注意到，若X是有限集，那么$A_i, i = 1, 2, 3, \cdots, n$是一个$X$的分类，这意味着

$$|X| = |A_1| + \cdots + |A_n|$$

3.6 命题

若$\equiv$是集合X上的一个等价关系，则等价类构成 X的一个分类，反之，给定X的一个分类P，则存在X上的一个等价关系，其等价类是P中的块

证明： 我们假设X上的一个等价关系$\equiv$给定，因为$\equiv$是自反的，所以每个$x \in X$位于等价类$[x]$中。所以等价类是非空的子集，为了证明两两不相交，我们设$a \in [x] \cap [y]$，则$a \equiv x$和$a \equiv y$，这意味着$x \equiv y$由引理3.4可知，$[x] = [y]$，所以每个等价类都是两两都是不相交的。所以等价类构成X的一个分类

反之，我们设P是X的一个分类，那么设$x, y \in X$，若存在$A \in P$有$x \in A, y \in A$。我们定义$x \equiv y$，显然$x \equiv y$满足自反和对称。为了证明传递，我们假设$x \equiv y$和$y \equiv z$，即存在$x \in A$和$y, z \in B$，因为$y \in A \cap B$，但A, B是两两不相交的，这意味着$A = B$，所以$x, z \in A$有$x \equiv z$。这是一个等价关系

最后我们要证明：等价类必须是P中子集，若$x \in X$，则对某个$A \in P$有$x \in A$，由等价定义，若$y \in A$则$y \equiv x$和$y \in [x]$因而$A \subseteq [x]$，对反包含我们设$z \in [x]$，那么$z \equiv x$存在某个B满足$x \in B$和$z \in B$，有$x \in A \cap B$，但$A \cap B = \emptyset$，所以$A = B$，有$z \in A$，$[x] \subseteq A$所以$[x] = A$

4 习题

4.1 判断题

1. 若$S \subseteq T$, $T \subseteq X$，则$S \subseteq X$
2. 任意两个函数$f : X \to Y$和$g : Y \to Z$ 都有一个合成$f \circ g : X \to Z$
3. 任意两个函数$f : X \to Y$和$g : Y \to Z$都有一个合成$g \circ f : X \to Z$
4. 对每个集合都有$X \times \emptyset = \emptyset$
5. 若$f : X \to Y$是一个函数，且存在函数$g : X \to X$满足$f \circ g = 1_Y$，则f是双射

解

1. 由于$S \subseteq T$，则$|S| \leq |T|$再由$T \subseteq X$有$|S| \leq |T| \leq |X|$，那么$S \subseteq X$对。
2. $f \circ g : X \to Z$，这意味着g输出Z，但X若存在不属于Z的元素，这意味着$f \circ g : X \to Z$是不成立的。所以错
3. 这次是考察$g(f(x))$的情况，由于$f : X \to Y$，这意味着f的值域刚刚好就处于g的定义域内并输出Z，是一个成功的映射，所以对于$x \in X$有$y \in Y$有$f(x) = y$，且存在$z \in Z$使得$g(y) = z$，那么$g(f(x)) = g(y) = z \subseteq Z$，所以$g \circ f : X \to Z$是成立的
4. 要验证这个命题，我们首先计算$X \times \emptyset$，$\emptyset$中不存在元素，这意味着形如$y \in \emptyset$的情况是不存在的，也就不能找到X中任何的非空子集构成一个非空的笛卡尔积，这意味着要使得$X \times \emptyset$的笛卡尔积只能是X中取出$\emptyset$，但什么都没有和什么都没有只能是没有，也就是$X \times \emptyset = \emptyset$。
5. 由定义2.9和引理2.10可知g是一个f的反函数，且f是单射和g是满射。再由命题2.11若f存在反函数g，当且仅当f是双射。所以命题成立。

4.2 证明题

1 设A, B都是集合，并设$a \in A,\ b \in B$定义如下有序对

$$(a, b) = \{a, \{a, b\}\}$$

若$a' \in A, b' \in B$，证明$(a', b') = (a, b)$当且仅当$a' = a$和$b' = b$

证明： 我们证明命题的逆否命题，假设$a' \neq a,\ b' \neq b$，那么$(a', b') = \{a', \{a, b\}\}$，这意味着$\{a\} \neq \{a'\}$而$\{a', b'\} \neq \{a, b\}$，所以$\{a, \{a', b'\}\} \neq \{a, \{a, b\}\} \Rightarrow (a, b) \neq (a', b')$所以假设不成立。所以$(a, b) = (a', b')$当且仅当$a = a', b = b'$

2 若$f : X \to Y$有反函数g，证明g是一个双射

由定义2.9，因为f具有反函数，那么就存在一个$g : Y \to X$使得$g \circ f = 1_X$，利用引理2.10可知f是一个单射且g是满射。且利用命题2.11得知f是双射。我们也假设g是一个双射，那么$x \in X$，因为f是一个双射，g是满射。所以$g : Y \to X$所以$\mathrm{im} g = Y$明显的存在一个唯一确定的$a \in X$使的$f(x) = y \in Y$是唯一确定的，因为g是f的反函数，又由于$f(x)$唯一确定，那么$g(f(x)) = x$也是唯一确定的，且对所有的$x \in X$都有$g \circ f = x$，所以g是双射。

3、鸽笼原理

1. 若X, Y都是有限集，且元素个数相同，对函数$f : X \to Y$证明下述条件是等价的
   (a) f是单射
   (b) f是双射
   (c) f是满射
2. 假设有11只鸽子，每只鸽子都在某个鸽巢中，若只有10个鸽巢，证明有一个鸽巢中鸽子数量超过1

证明

对于命题b，我们假设命题a是成立的，那么由于f是单射，这意味着对于每个$x \in X$，都有一个$f(x) = y \in Y$是唯一确定的。为此由于$|X| = |Y|$并且f是单射，那么$\mathrm{im} f = Y$，f是双射。现在，因为f是双射，那么

每个$f(x) = y$都是唯一确立的，又因为$|X| = |Y|$，所以f是一个满射。因为f是满射，所以f至少存在一个$y \in Y$有一个$x \in X$对应。因为$|X| = |Y|$所以f是单射。所以三个命题是互相等价的

对于问题2，利用命题1的证明，我们知道有，每个鸽子都必须至少有一个笼子，所以10只鸽子都至少占用了10个鸽巢，但鸽子数量是11，所以至少有一个巢存在2只鸽子