抽象代数学习笔记（一）

这几日恰巧在自学离散数学的内容，发现了一些很有趣的想法，加之下学期学业可能更加繁忙，故将原本打算于下学期开始更新的笔记提前至假期中撰写。

在笔记开始前，先声明一下：本笔记将会包含抽象代数与组合数学两部分的内容。其中抽象代数部分的内容将比较基础（Galois 理论这种的就不存在了 233，若之后有时间可以另行补充）。另外，假定读者都具有了集合论的基本知识（很多符号在第一次出现时，将会略做解释所以不用太担心符号问题）。

与初等数论笔记类似地，在每章笔记末尾，我将放一些我自认为有趣或者有价值的练习题并且给出我的解答以供大家参考。（数值分析以及概率论的习题有空会补上，再次挖坑 233）

更新：

我还是决定把名字换回抽象代数了 2333（因为突然发现自己不得不重新过一遍抽代一些比较深入的内容，所以应该还是能算得上是一个比较完整的抽代系列笔记的）

至于组合数学的内容，之后会额外地补上（个人感觉就比较轻松愉快了 233）

在正式开始前，我们对于抽象代数略作介绍。

抽象代数的主要研究对象是一类代数系统，而非特定的代数系统。我们学习的数学分析建立在实数域  上，复分析建立在复数域  ，而初等数论建立在自然数域  上。然而，抽象代数不关注特定代数系统本身的性质，转而关注具有类似性质的代数系统所共有的性质。从这个角度而言，其抽象层次提升了许多，很多定理的含义不再那么容易理解。

我个人比较倾向于从实例与形式两方面同时理解定理的含义。仅仅从实例理解，难免忽略结论的普遍性，拘泥于特定代数系统之中；仅仅从形式上理解，难以体会到数学知识的美妙之处，且不便于记忆。故两者结合才能取得良好的学习效果。

离散数学系列笔记的前言就到此为止。

提及代数系统，读者能很自然地想到其作用就是进行代数运算。代数运算既需要用来进行运算的“数”，即某个特定集合  中的元素，又需要数之间进行的运算法则，即集合  到自身的映射。

由此，我们引入

元运算的定义。

定义：

一个

的函数被称为集合 上的 元运算。

特别地，我们常用到的二元运算将

中的有序对 映射到一个 中元素 。我们常常用到的特殊代数常数 可以看作是零元运算 ，将所有元素都映射到这个常数。（ 表示集合论中的有序对）

我们常常用

表示 元运算，对于二元运算，可以简写为 ；对于一元运算，可以记作 。

为了进一步研究二元运算，我们定义一些二元运算可能具有的良好性质。

定义：

单个二元运算性质：

运算具有交换律：若满足

运算具有结合律：若满足

运算具有幂等律：若满足

两个二元运算之间的性质：

运算对于 运算具有分配律：若满足

运算和 运算具有吸收律：若这两个运算均可交换，且

（注意吸收率律的前提是都满足交换律）

对于二元运算的研究除去运算本身的性质之外，还能利用集合中关于运算的特殊元素来研究。

定义：

若

 ，则  为幂等元。

若

 ，则  为左幺元（左单位元）。

若

 ，则  为右幺元（右单位元）。

若

 同时为左幺元、右幺元，其为幺元（单位元）。

若

 ，则  为左零元。

类似地，我们可以定义右零元。

若

 同时为左零元、右零元，其为零元。

进一步地，若幺元

 存在，且  ，则  为  的左逆元。

类似地，我们可以定义

 的右逆元。

若

同时为 的左逆元、右逆元，其为 的逆元，记为 。

与逆元紧紧相关地，我们定义运算的消去律。

定义：

不为零元，若从 可以推出 ，且从 可以推出 ，则运算满足消去律。

我们定义了那么多的运算性质以及特殊元素，那么从这之中我们能够得到些什么有趣的结论呢？

一个有趣的结论是关于幺元的。

下面若无特别说明，认为

为 上二元运算。

定理（幺元的存在唯一性）

若

，则 为幺元且唯一。

证明：

容易发现

为左幺元， 为右幺元。他们在特定的一侧与任意元素运算都将保持元素不改变。由此，我们不妨看看 会发生什么。

发现

（ 右幺元），（ 左幺元）

故有

，同时为左右幺元，自然为幺元且唯一（唯一性可模仿上述过程反证）。

上述定理向我们展示了一个代数结构中幺元的性质：若存在必唯一，且不同的左右单侧幺元不能同时存在。我们发现：这个结论是纯粹依靠我们的定义推出的，并无借助到任何其他的性质，这是幺元自定义本身就带有的一种结构。

类似地，我们有零元的存在唯一性定理，由读者自行完成。

然而，对于逆元，其存在唯一性并不能被定义直接保证，我们将会需要一些额外的条件。

关于幺元、零元、逆元的其它性质将会在习题中展示。

关于运算的性质，我们看一具体例子。

例：考虑正整数集

 ，以及其上两个二元运算  （求最大公因数）与  （求最小公倍数）。

首先，

 与  运算在  上是封闭的。

其次，我们容易发现这两个运算具有交换律、结合律、幂等律、分配律以及吸收律，但是显然没有消去律（证明略去）。

对于特殊元素，我们发现

 ，故  为  的零元。

类似地，

 ，故  为  的幺元。

在有了运算的定义之后，我们就能够严格定义代数系统的概念。

定义：

代数系统

 ，其中  为非空集合，称为载体；  为所有  元运算的集合；  为代数常数集合（  元运算）。

如：

 均为代数系统。

通常而言，代数系统也可记为

，其中 均表示运算。

代数系统的一个经典实例是字代数以及语言代数，将在下一章中提及。

对于两个代数系统之间的关系，我们引出一些简单的定义。

定义：

若

，两个运算对应地有相同元数，则称两个代数系统同类型。

若

，且对应运算，相等，则称 为 的子代数。

进一步地，若

为 的子代数且 （ 为所有零元运算集合）或 成立，则此子代数为平凡的，否则为非平凡的。

例：

表示将 中每个元素乘以 后组成的集合。则 为 的子代数。特别地， 时子代数为平凡的，否则为非平凡的。

对于代数系统研究的一个问题是：我们所接触到的不同代数结构终究是有限的。要如何通过已有的代数系统构造新的呢？积代数为我们提供了一种简单的方法。

定义：

为同类型代数系统， 均为 元运算。积代数 满足性质

，且  称为因子代数。

读者可能感觉这个定义十分复杂，但是本质上只是告诉了我们一个很简单而自然的构造方法：有序对的运算结果定义为对不同分量分别的运算结果组成的有序对即可。

这样的构造方法事实上并没有破坏原来运算的性质与结构，而只是进行了简单的分量组合，所以

 运算的很多良好性质得以保留至  上。

定理（积代数保持运算性质）

对于原先的运算

 ，其具有的交换律、结合律、幂等律能够保持至  。

若两组运算

 以及  之间均有分配律、吸收律，则能够保持至  之间。

进一步地，若因子代数幺元分别为

 ，则  为积代数的幺元（零元、逆元也均能够保持）

定理的证明只需要简单利用定义即可。

但是值得注意的一点是：积代数不能保持消去律！

消去律作为一项有些特别的性质，需要特别注意！

反例：

，其中  表示  可能的余数组成的集合（  ），  为  意义下的乘法。

容易验证这两个代数结构上均有消去律，但是考虑

 中的元素

显然不满足消去律。

接下来，我们给出代数系统同态与同构的定义。

定义：

为同类型代数系统，  均为  元运算。若存在函数  ，使得对于  ，有

成立，则  为代数系统  到  的同态。

特别地，若

 为满射，称为满同态，记作  。

若

 为单射，称为单同态。

若

 为双射，称为同构，记作  。

若

 ，称  为自同态。类似地，可以定义自同构。

从同态的定义出发，能够保持代数系统运算的函数就是一种同态。同态需要满足的性质是在

 中先运算完后再取函数像等于先取函数像后再于  中进行运算。某种程度上而言，同态保证了两种代数结构在各自运算下的相似性。

同构则是更加严格的。其在同态的基础上添加了一一对应的条件，保证了两个代数结构的载体必定等势。同构的代数系统在抽象意义下可以认为是完全相同的。

如：

均为代数系统。

我们不难发现这两者是同态的，且存在

到 的单同态。这意味着在 上的加法与在 上的加法具有类似的性质。然而，由集合论知识，显然不存在同构。这意味着两个代数系统仍旧存在着差别，载体中的元素不能做到一一对应。

注意到同态保持代数系统运算的性质，我们发现：利用同态也能很容易地构造出子代数。

同态的性质恰巧保证了其像集对于运算的封闭性。

故我们定义：

为同类型代数系统， 均为 元运算。若存在函数 为代数系统 到 的同态，则 必为代数系统，且为 的子代数。 被称为 在 下的同态像。

与积代数类似地，同态像继承了运算的良好性质。然而，消去律仍然是一个例外！反例由读者自行给出。

最后，我们介绍商代数。

首先，为了之后的便利，先介绍一种特殊的等价关系：同余关系。

定义：

， 均为 元运算。 为 上等价关系。

若满足

，

，则 对于 具有置换性质。

若

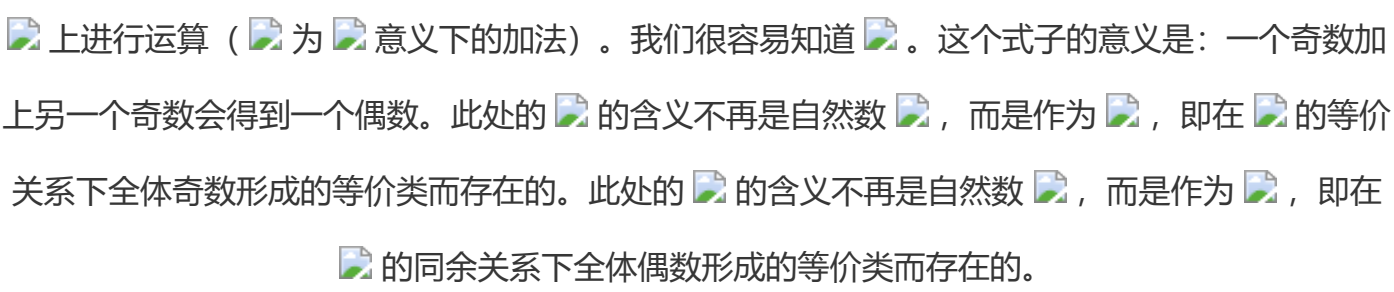
对于 的所有运算都具有置换性质，称其为 上同余关系。

同余关系的内涵可以简单地概括为：每个参与运算的元素对应等价，则最终运算的结果也等价。这为之后引入商代数奠定了良好的基础。

在引入商代数之前，我们回忆等价关系的相关知识。等价关系的最常见应用就是进行分类。由于自反性、对称性、传递性，等价关系可以保证将一个集合中的所有元素分成不漏、不重的数类。这意味着：等价关系诱导了原集合的一个划分。

商代数被定义的动机就是将代数运算进一步地抽象一个层次。我们可以不再拘泥于对集合中的元素进行运算，转而对等价类进行运算。商代数的运算对象不再是载体中的元素，而是载体中的所有元素被等价关系诱导而形成的若干个类别。

商代数在这一点上与同余意义下的运算很相似。例如在



上进行运算（ 为 意义下的加法）。我们很容易知道 。这个式子的意义是：一个奇数加上另一个奇数会得到一个偶数。此处的 的含义不再是自然数 ，而是作为 ，即在 的等价关系下全体奇数形成的等价类而存在的。此处的 的含义不再是自然数 ，而是作为 ，即在 的同余关系下全体偶数形成的等价类而存在的。

理解这一点至关重要！我们再一次进行归纳：对于载体中元素按照等价关系划分为等价类。商代数将每一个等价类看成一个元素而忽视等价类内部的元素的差别进行运算。商代数的运算数是原载体的等价类，运算结果也是原载体的等价类。

定义：

， 均为 元运算。 为 上同余关系。

关于同余关系 的商代数记作 （ 表示 关于同余关系 的商集）。商代数中的运算定义为：

。

简单地理解：等价类之间的运算等同于先对等价类的代表元进行运算后再取等价类。

读者阅读至此可能会产生一个疑问：这样定义的运算真的合理吗？会不会发生选取同一等价类中不同代表元导致运算结果不同的现象呢？这是一个很好的问题。是我们在定义商代数时所必须要考虑到的良定义问题。其含义是：运算结果仅仅与等价类有关，而与等价类中代表元的选取无关。到这里，读者可能已经发现我们之前将等价关系加上置换性质变成同余关系的动机所在：使得商代数具有良定义的性质。（简单的证明，读者自证）

与积代数类似地，商代数仍旧能够保持大部分运算的良好性质（定理略），但是消去律依旧还是个例外。

现在，我们再来回顾刚刚所举之例：

 。

我们现在来构造代数系统

 以及同余关系  ，使得  。

由于

 将所有整数分为了奇偶两类，我们不妨尝试  ，同余关系  定义为  。

容易验证

 为代数系统，  满足自反性、对称性、传递性。

对于

 ，若  ，则  ，故满足置换性质，即  在  上为同余关系。

故我们可以求出由同余关系诱导出的划分。其将所有整数划分为奇数与偶数两大类。

不妨设奇数的等价类为

 ，偶数的等价类为  ，则  。

进一步地，运算

 被定义为  ，  ， 

与

 意义下的加法完全一致。由此，我们证明了  。

最后，我们探讨一些同态与商代数之间的有趣而重要的联系。

我们先探究同态与同余关系之间的对应。

定理（同态诱导同余关系）：

为同类型代数系统，  均为  元运算。若存在函数  为代数系统  到  的同态，则由同态可诱导出

 上的同余关系：  。

证明：

容易发现

 满足自反性、对称性、传递性，故为等价关系。

则只需证明其对每个运算都满足置换性质。

取

则考虑

 ，利用同态保持运算的性质，得到

故

，得证。

上述定理告诉我们：给定一个同态，必定可以由其诱导出一个同余关系，从而诱导出一个对应的商代数。

很自然地，我们会问：那么给定一个商代数，我们是否能够从同余关系诱导出一个对应的同态呢？

定理（同余关系诱导同态）

 ，  均为  元运算，  为  上的同余关系，则  同态于  。

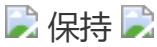
证明：

为了证明同态关系，我们需要构造同态映射。

回忆在定义商代数中的运算时，我们定义等价类的运算结果等于代表元运算后再取等价类。所以在这里，我们用到自然同态作为同态函数。

 满足 ，其将 中元素映射到其对应的等价类。

由商代数的运算定义，我们容易证明此处的

 保持 中所有运算，故为同态。

上述定理告诉我们：给定一个商代数，由其同余关系，我们必定可以诱导出一个自然同态将载体中元素映射到其对应等价类中。

这两个定理告诉我们：同态与同余关系是紧密联系的，是可以相互诱导的。

最后，我们给出至关重要的同态基本定理。

定理（同态基本定理）

为同类型代数系统，  均为  元运算。若存在函数  为代数系统  到  的同态，且  为由  诱导出的  上的同余关系。则  。

证明：

要证明同构，需要构造函数

 。

一个很自然的构造就是将等价类映射到其代表元在同态下的像。

即

 。

假设商代数

那么

故

 保持运算，为同态。

进一步地，对于

 中每个元素，在  中都能找到原像，故  为满的。

若

 ，则  ，则  ，故  。

故

 为单的。

所以

 为双射，  。

同态基本定理告诉我们：任何代数系统的商代数都是自己的一个同态像。反之，任何代数系统的同态像必定是自己的一个商代数。同态与同余关系、同态像与商代数，都是统一的，本质是相同的。

习题：

1、

 中至少有两个不同元素，且幺元与零元都存在。证明：幺元必不等于零元。

2、

 为代数系统，  有结合律，幺元存在。证明：若对一元素左右逆元都存在，则其逆元存在唯一。

3、 证明代数系统

恰好存在 个自同态。

4、

，找到 上所有同余关系（用等价类表示）。

5、

，其中 为二元运算。在积代数 上定义同余关系：

。证明： 。

提示或解答：

1、反证即可。

2、利用运算结合律，考虑

即可， 分别为左右逆元。

3、

这道题乍看上去让人摸不着头脑，但是我们进行一些尝试就能够发现规律。

首先不妨假设

为自同态。由于 为幺元，根据同态的性质， 也应该为幺元，故 。

我们不妨观察一下

，其中有 三个元素。

考虑

，其中仅有元素 ，同态于 。

而

 中有元素 ，化简得到 ，显然也是一个同态。

我们由此发现：

 ，  均为同态函数。

读者容易自行证明其保持了运算，为同态，且相互不同。

由此，我们找到了

 个不同自同态。

我们只需要证明：对于其它自同态，必为上述

 个之一。

我们不妨假设

 。则只需要证明  即可。

（利用数学归纳法易证）

这道习题向我们清晰地展示了

 的代数结构，其本质上是一个有限循环群。

4、

注意到每个同态可以诱导出一个同余关系，我们只需要对于每个不同同态求出其对应的同余关系即可。

我们利用第三题中结论。恰好有

 个不同同态。

通过计算我们可以发现：

 将所有元素映射到  ，故诱导出的同余关系的对应等价类为  。

诱导出的同余关系的等价类为

诱导出的同余关系的等价类为

诱导出的同余关系的等价类为 。

由此，我们发现：不同同余关系共有

个。

5、

要证明商代数与另一个代数结构同构，不妨利用同态基本定理。

为了凑成同态基本定理的形式，我们将

作为同态像， 作为由同态映射诱导出的同余关系。

由此，我们可以定义

，使得其将 映射到 （ ）

则

故

为同态函数。

我们发现如此定义出的同态

恰好诱导出了同余关系 。

由同态基本定理，

而我们发现对于任意

 中的元素，都存在关于  的原像，故其为满同态。

故

 ，得证。

关于第一部分的内容就到此为止，谢谢各位的阅读！

全文完