研究生数学系列规划教材

抽象代数释议

冯克勤　廖群英　著

机械工业出版社
CHINA MACHINE PRESS

研究生数学系列规划教材

抽象代数释议

冯克勤　廖群英　著

机械工业出版社

本书通过对三十一道习题（精选自作者三十多年来在中国科学技术大学和清华大学讲授抽象代数及其应用方面的课程时积累下来的题目）的详细解释和议论、以及发散的讨论，阐述对抽象代数的认识，以及如何教好和学好抽象代数的问题。本书可作为高年级本科和研究生课程的辅助教材，更可作为教学参考用书。

图书在版编目（CIP）数据

抽象代数释议/冯克勤，廖群英著．—北京：机械工业出版社，2009.5
（研究生数学系列规划教材）
ISBN 978-7-111-26408-8

Ⅰ．抽…　Ⅱ．①冯…②廖…　Ⅲ．抽象代数—研究生—教材　Ⅳ．0153

中国版本图书馆 CIP 数据核字（2009）第 025046 号

机械工业出版社（北京市百万庄大街 22 号　邮政编码 100037）
责任编辑：韩效杰　版式设计：霍永明　责任校对：陈延翔
封面设计：鞠　杨　责任印制：洪汉军
三河市国英印务有限公司印刷
2009 年 5 月第 1 版·第 1 次印刷
169mm×239mm·9.75 印张·131 千字
标准书号：ISBN 978-7-111-26408-8
定价：19.80 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
销售服务热线电话：（010）68326294
购书热线电话：（010）88379639　88379641　88379643
编辑热线电话：（010）88379408
封面无防伪标均为盗版

引　言

抽象代数是大学数学系本科生的必修或选修课程。近年来，研究生开设此课程的要求也有增加的趋势。抽象代数（或叫近世代数）不仅是研究数学各领域的重要代数工具（数论、代数、微分几何、数理方程、计算数学、控制理论与组合数学等），也是计算机科学和信息科学等应用领域的数学工具。就目前我国高校数学教育的现状而言，本科学习期间的抽象代数训练不够充分，所以为研究生开设抽象代数课程是很有必要的。

目前，国内外已有许多抽象代数的好教材，与几何拓扑学相比，高校的代数学教员也不算缺乏，根据与高校老师和研究生的多年接触，笔者感到当前国内抽象代数教育的主要问题是教与学的内容和方法，即哪些是抽象代数最本质的东西，哪些是老师应当教给学生，而学生最需要学会的。

抽象代数产生于19世纪，那是代数学发展的一个重要阶段。1930～1931年范德瓦尔登（Van der Waerden）的《Morden Algebra》一书是抽象代数的经典著作，后来多次再版，书名改为《Algebra》，去掉了“Modern”（近世的，或叫摩登的）一词。1980年N. Jacobson的书中讲述了比传统抽象代数更为丰富的内容，而书名叫作《基础代数》（Basic Algebra）。这表明，半个世纪之前还认为很现代或很抽象的代数，现已成为基础知识。尽管如此，大学生或者研究生在第一次学习抽象代数时，多数学生还是感到很抽象的。与他们学过的数学课程相比，在内容特别是风格上有很大不同，所以如何教好和学好抽象代数，是一个突出的问题。

抽象代数研究群、环、域这些代数结构的一般性质，所以首要的一件事情是一定要有大量的例子。老师通过例子向学生展示这些代数结构所蕴涵的生动现实、历史溯源和应用威力，学生通过例子

把握所学内容的实质，体会定理结论和证明的真实含义。形式逻辑的推导是这门课程的重要训练内容，但只是骨架。而具体生动的例子是其中的血肉。其次，抽象代数这门课程非常鲜明地体现了数学的特点，即特殊与一般、具体与抽象的关系。要学会从大量特殊的具体的例子中抽象出普遍性质的能力，学会在相互比较和联系（即群和环的同态）当中研究代数结构的能力，学会在心中有真实背景的基础上进行形式逻辑推理的能力。而培养学生的这些能力也正是老师的教学重点，这些能力的培养对于学习数学的研究生无疑是非常重要的。

第一作者从1970年代起，在中国科学技术大学和清华大学讲授抽象代数，也给研究生（包括信息和组合学专业的研究生）讲过抽象代数及应用方面的课程。在这里，我们挑选了教学中曾经使用过的31道习题，加以解释和议论，以这些题目作为具体例子，来阐述对抽象代数的认识，说明对讲授和学习这门课程的一些看法，供诸位同仁参考和指正。

本书题目的分类并不是按讲课的次序，而是按知识和能力的训练特点分类。第一章是群、环、域的基本概念，通过例子加强对基本概念的理解。第二章是各种代数结构的一般性质和特殊性质，强调用相互比较和联系的手法研究代数结构。注重使用同态手段，这是抽象代数的核心。第三章是抽象代数在组合设计与信息科学中的一些应用，这些题目大都源于某些数学游戏，但有着深刻的应用背景。所用的代数结构主要是有限域，但在解决问题中广泛采用了抽象代数的思考方法和手段，而不是简单的使用抽象代数的某些结论，这种训练对于应用领域的研究生是重要的。

机械工业出版社对于出版这本书给予了热情的支持，在此深表感谢。

冯克勤　廖群英（于清华园）

目　录

第一章　基本概念和例子

习题 1.1　设 S 是含幺半群。证明：S 中所有可逆元素对于 S 中的运算形成群。

【释议】　一个非空集合 S 叫做**半群**，是指 S 中存在一个满足结合律的二元运算

$$S\times S\to S,\quad (a,b)\to a\cdot b。$$

如果 S 中有元素 e，使得对每个 $a\in S$，均有 $ea=ae=a$，则称 S 为**含幺半群**，e 叫做半群 S 中的**幺元素**。半群 S 与运算“$\cdot$”有关，所以更准确地应把半群记成$(S,\cdot)$，在运算不发生混淆时，简记为 S。

一个含幺半群 S 称为**群**，是指对每个元素 $a\in S$，均有 $b\in S$，使得 $ab=ba=e$。b 叫做 a 的**逆元素**，记成 $b=a^{-1}$。

学生在看到习题 1.1 的时候，不少学生不知道要证什么，认为这是不需要证明的。设 $U(S)$ 是含幺半群 S 的可逆元素全体构成的集合。根据定义，含幺半群中如果每个元素都有逆，它就是群。现在 $U(S)$ 中既然都是可逆元，那不就是群吗？

事实上，这是一个考察是否真正理解群概念的题目，需要证明的事情是很多的。

(1) 首先证明 S 中的运算也是子集合 $U(S)$ 中的二元运算，即若 a 和 b 属于 $U(S)$，则 ab 也属于 $U(S)$。这相当于要证明：若 a 和 b 均是 S 中的可逆元素，即存在 $a',b'\in S$，使得

$$aa'=a'a=e,\quad bb'=b'b=e,$$

则 ab 也是 S 中的可逆元素。我们并没有假定 S 中运算满足交换律，同学在线性代数中已经熟悉矩阵乘法运算不满足交换律，并且知道当两个 n 阶实方阵 $\boldsymbol{M}$ 和 $\boldsymbol{N}$ 可逆时，$\boldsymbol{MN}$ 也可逆，并且$(\boldsymbol{MN})^{-1}=\boldsymbol{N}^{-1}\boldsymbol{M}^{-1}$，所以从这个经验他应当猜测 ab 是可逆的，并且逆应当为

$b^{-1}a^{-1}=b'a'$，而且要学会下面形式化的证明：

根据运算的结合律，可知

$$(ab)(b'a')=a(bb')a'=(ae)a'=aa'=e,$$

$$(b'a')(ab)=b'(a'a)b=(b'e)b=b'b=e,$$

因此$(ab)^{-1}=b'a'=b^{-1}a^{-1}$。这表明 S 中的二元运算也是 $U(S)$ 中的二元运算。

(2) 运算“·”在 $U(S)$ 中满足结合律，这一点确实是显然的，因为运算在 S 中如此，当然在 $U(S)$ 中也如此。

(3) $U(S)$ 中有幺元素 e，从而 $U(S)$ 是含幺半群。

(4) 根据群的定义，对于 $U(S)$ 中每个元素 a（即 a 是 S 中可逆元素），a 在 $U(S)$ 中要有逆元素。我们前面给出的 $a^{-1}=a'$ 只是属于 S，所以还应当证明 $a^{-1}\in U(S)$。换句话说，我们需要证明：若 a 是 S 中可逆元（即 $a\in U(S)$），则它的逆元素 $a'=a^{-1}$ 也是可逆元（即 $a^{-1}\in U(S)$）。证明也不难：由 $aa'=a'a=e$ 可知 a 是 $a'=a^{-1}$ 的逆元素，即 $(a^{-1})^{-1}=a$。

这就证明了 $U(S)$ 对于 S 中的运算是群。证明的每一步都不难，关键在于弄清楚需要证明什么，在刚开始学习抽象代数的时候，这种准确地把握定义本质并严格地进行形式化推理，是一种必要的训练。

我们不主张给学生讲述许多关于群的等价定义，那会把学生搞烦，人为地把事情复杂化。但是要指明：半群 S 中若存在幺元素 e，则幺元素是唯一的，即若 $e,e'\in S$，并且对每个 $a\in S$，均有

$$ea=ae=e,\quad e'a=ae'=e',$$

则必然 $e=e'$。要使学生知道考虑 ee'。由于 e 是幺元素，取 $a=e'$ 可知 $ee'=e'$，又由 e' 是幺元素可知 $ee'=e$，于是 $e'=ee'=e$。同样地要指明：如果 a 在含幺半群 S 中可逆，则 a 的逆元素也是唯一的，所以才能表示成 a^{-1}。证明对于初学者也是一个很好的形式化练习：设 b 和 c 都是 a 的逆元素，考虑 bac，一方面它为 $(ba)c=ec=c$，另一方面它为 $b(ac)=be=b$。因此 $b=c$，即 a 的逆元素是唯一的。

习题 1.2　试问非交换群的最小阶数 n 是多少？n 阶非交换群不计同构是否唯一？

【释议】　这个问题我们多次用来作为研究生入学的口试题，通过相互问答和讨论，可以看出学生对于群的理解程度。多数学生知道素数阶群为循环群，并且知道这种循环群的例子：整数模 p 的加法群 $Z_p=\mathbb{Z}/p\mathbb{Z}$（其中 p 为素数），所以 1，2，3，5 阶群都只有 1 个循环群，它们是交换群。学生应该知道 4 阶群只有两种：Z_4 和 $Z_2\times Z_2$，并且应当说清楚为什么它们不同构。在这里可以进一步问：如果一个有限群 G，除了幺元素之外每个其他元素的阶都是 2，这个群是否为交换群？好的学生应当知道答案是肯定的，而且能够给出证明：对于 G 中每个元素 a 和 b，$a^2=b^2=(ab)^2=1$。于是 $a=a^{-1}$，$b=b^{-1}$，$ab=(ab)^{-1}=b^{-1}a^{-1}=ba$，所以 G 是交换群。

接下来考虑 6 阶群。掌握得好的学生应当知道 6 阶交换群只有一个：Z_6。也就是说，要知道加法群 $Z_2\times Z_3$ 和 Z_6 同构，而且应当知道 6 阶非交换群的例子：三元集 $\{1,2,3\}$ 的全部置换组成的对称群 S_3，它是非交换群：$(12)(13)=(132)$，$(13)(12)=(123)$。或者知道几何上的例子：正三角形的对称群 D_3，由三个旋转和三个反射组成，而且知道 S_3 和 D_3 同构，这只需把正三角形的每个对称等同于三个顶点的置换即可看出，所以，非交换群的最小阶数是 6。

于是来到最后一个问题：6 阶非交换群是否只有一个？一个优秀的学生应该通过推导给出答案。设 G 是 6 阶群，则 G 中元素的阶为 1，2，3 和 6（拉格朗日定理）。如果 G 中有 6 阶元素 a，则 G 就是由 a 生成的循环群。否则，G 中每个元素（$\neq e$）的阶为 2 或 3，并且 G 是非交换群。这时 G 必有 3 阶元素。因为我们已经知道，若 G 中每个元素（$\neq e$）的阶都是 2，G 必然是交换群。进而，若 G 中每个元素（$\neq e$）的阶都是 3，则 G 中除 e 之外，其余元素均成对 $\{a,a^{-1}\}$ 出现（这是因为如果 $a^2\neq e$，则 $a\neq a^{-1}$），从而 G 的阶数为奇数，和 G 的阶数为 6 相矛盾。所以除了幺元素 e 之外，必还有 $b\in G$ 使得 $b^2=1$。b 就是 2 阶元素。

于是在 6 阶非交换群 G 中，同时存在 2 阶元素 b 和 3 阶元素 a，

然后可知 G 有 3 阶子群 $H=\{e,a,a^2\}$，并且 G 对于 H 有两个陪集

$$G = H \cup bH = \{e,a,a^2,b,ba,ba^2\},$$

元素 ab 不可能是 e,a,b 和 a^2，所以 $ab=ba$ 或 $ab=ba^2$。如果 $ab=ba$，则 G 是由可换的两个元素 a 和 b 生成的群，G 必是交换群，所以若 G 是非交换群，必然 $ab=ba^2$。这个关系决定了 G 中所有 6 个元素运算的乘法表。这就表明 6 阶非交换群只有一种结构。或者考虑映射

$$\varphi : G \to S_3, \quad \varphi(a) = (123), \quad \varphi(b) = (12),$$

由 a 和 b 分别是 3 阶和 2 阶元素以及关系式 $ab=ba^2$，可证 φ 是群的同构，即每个 6 阶非交换群都和 S_3 同构。

习题 1.3　三维实空间$\mathbb{R}^3$中有多少欧氏变换，可以把其中的一个固定的正立方体变成自身？

【释议】　将一个固定的正立方体保持不变的全部欧氏变换（欧氏运动）形成一个群，两个变换 A 和 B 的乘积 AB 为变换的合成（先作用 B 然后作用 A）。幺元素即为恒等变换（每点均不动）。由于正立方体有 8 个顶点（如图 1-1），

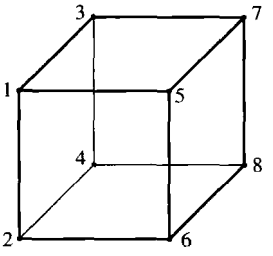

图　1-1

每个变换可以等同于这 8 个顶点的置换，所以这个变换群 G 可以等同于 S_8 的一个子群。我们的问题是求出群 G 的阶。杂乱无章地计算很难把 G 中元素找全，采用群论的思考方式通常是最有效的。

考虑 G 中将顶点 1 固定不动的那些变换，它形成 G 的一个子群 H。子群 H 很容易计算，因为若顶点 1 不动，与顶点 1 相邻的三个顶点 2,3,5 也必然变成与顶点 1 相邻的顶点，即要把$\{2,3,5\}$变成自身，则变换为以顶点 1 为中心旋转，如果顶点 2 变为 5，则 5 必变到 3，而 3 变到 2。相应地，顶点 6,7,4 分别变为 7,4,6。而顶点 8 保持不动，所以这个变换就是顶点之间的置换(253)(674)。H 是由它生成的 3 阶子群：

$$H = \{I,(253)(674),(235)(647)\},$$

G 对于子群 H 分解成一些陪集的并集：

$$G = \sigma_1 H \uplus \sigma_2 H \uplus \cdots \uplus \sigma_l H,$$

其中 $\sigma_i \in G(1 \leqslant i \leqslant l)$，记号$\uplus$表示陪集 $\sigma_i H(1 \leqslant i \leqslant l)$彼此不交，即它们是不同的陪集。对于 G 中任意一个置换 τ，

$$\begin{aligned}\tau \in \sigma_i H &\Leftrightarrow \tau = \sigma_i h (h \in H)\\ &\Leftrightarrow \sigma_i^{-1}\tau = h \in H\\ &\Leftrightarrow (\sigma_i^{-1}\tau)(1) = 1 \quad (\text{因为 } h \text{ 固定顶点 } 1)\\ &\Leftrightarrow \tau(1) = \sigma_i(1),\end{aligned}$$

这表明，若 $\sigma_i(1)=s(1\leqslant s\leqslant 8)$，则陪集 $\sigma_i H$ 就是 G 中所有把顶点 1 变成 s 的那些置换所构成的集合，所以陪集的个数 l 就是顶点 1 由 G 中置换可以变成的顶点个数。容易看出顶点 1 经过 G 中某个置换可以变成正立方体的任何一个顶点（这叫做群 G 在正立方体的顶点集合 $\{1,2,\cdots,8\}$ 上是可传递的），所以 G 对于 H 共有 8 个陪集，即 $l=8$，于是 $|G|=8|H|=3\cdot 8=24$。对每个顶点 $s(1\leqslant s\leqslant 8)$ 取一个置换 σ_i 将 1 变成 s（例如可取 $\sigma_1=I,\sigma_2=(1234)(5678)$ 等等），可把每个 $\sigma_i H$ 中的 3 个置换具体写出，然后便可把 G 中 24 个置换全部写出来。我们也可把 G 中每个变换看成是正立方体六个面 A,A',B,B',C,C' 的置换，其中 A 和 A' 分别为前后面，B 和 B' 分别为左右面，C 和 C' 分别为上下面（如图 1-2）。

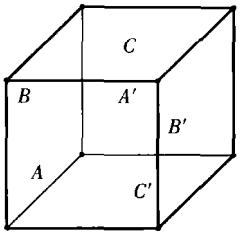

图　1-2

将 A 面不动的所有变换形成 G 的一个子群 H'，H' 中元素也把 A' 面保持不动，而另四个面依次旋转，因此 H' 是由面上置换 $(B'C\ BC')$ 生成的 4 阶循环群。群 G 在六个面上的置换作用是可传递的，所以 G 对于子群 H' 有 6 个陪集，于是也可算出 $|G|=6\cdot|H'|=6\cdot 4=24$，所以 G 也同构于 S_6 的一个 24 阶可传递子群。

最后，G 也可看成是正立方体 12 条边上的置换群。将每条边不变的置换形成 G 的一个 2 阶子群 H''，G 在边集合上是可传递的，从而

G 对于 H'' 共有 12 个陪集，又算出 $|G|=2\cdot 12=24$，并且 G 同构于 S_{12} 的一个可传递子群。

置换群是一类重要的群，这是因为每个 n 阶有限群 $G=\{g_1, g_2, \cdots, g_n\}$ 均可看成集合 G 上的一个置换群。方法是：对于每个 $g\in G$，考虑集合 G 上的一个置换

$$\sigma_g : G\to G,\quad \sigma_g(g_i)=gg_i(1\leqslant i\leqslant n),$$

验证 σ_g 是集合 G 上的置换（即 $\sigma_g(g_i)=\sigma_g(g_j)\Leftrightarrow g_i=g_j$）。并且对于 $g,h\in G$，有

$$\sigma_g\sigma_h=\sigma_{gh},\quad \sigma_g^{-1}=\sigma_{g^{-1}}。$$

由此可知 $G'=\{\sigma_g\mid g\in G\}$ 形成群，它是 G 上所有置换形成的对称群 S_n 的子群，由 $\sigma_g\sigma_h=\sigma_{gh}$ 可知映射

$$G\to G',\quad g\mapsto\sigma_g$$

是群的同构。这就表明：每个 n 阶有限群都可看成是对称群 S_n 的子群，所以置换群是群的一种样板。这个结果固然很漂亮，但是当 $n=|G|$ 很大时，S_n 是阶数（$=n!$）很大的群。我们希望 G 能做成是 S_m 的子群，其中 m 愈小愈好。比如对于正立方体的 24 阶对称群 G，看成正立方体六个面的置换，G 可看成 S_6 的子群，S_6 比 S_{24} 的结构要简单。

另一类样板群是域 K 上 n 阶可逆方阵构成的乘法群，叫做域 K 上的 n 阶一般线性群（general linear group），表示成 $GL(n,K)$，其中 n 为任意正整数，K 可以是任意域。这些群来源于线性代数。

有限循环群的样板是 $(Z_n,+)$，有限交换群的样板是乘法半群 Z_n 中可逆元构成的乘法群 $(Z_n^*,\cdot)$，其中 Z_n 的乘法可逆元全体为 $\{\bar{a}\in Z_n\mid a$ 和 n 互素$\}$。乘法群 Z_n^* 的阶为欧拉函数 $\varphi(n)$，它定义为 1，2，…，n 当中与 n 互素的数的个数，无限循环群均同构于整数加法群 $\mathbb{Z}$，这些群来源于初等数论。以上这些群的例子是同学应当熟悉的。

习题 1.4　*决定整数加法群$\mathbb{Z}$和有理数加法群$\mathbb{Q}$的自同构群。决定n元循环群的自同构群。*

【释议】　群G到自身的同构叫做群G的自同构。群G的所有自同构对于合成运算成群，表示成$\mathrm{Aut}(G)$，幺元素为恒等自同构I。一般来说，决定一个群的自同构群是群论中一个困难的问题。但是对于习题中所列的简单群，可以完全决定他们的自同构群。

首先考虑整数加法群$(\mathbb{Z},+)$。设σ是加法群$\mathbb{Z}$的一个自同构，$\mathbb{Z}$的幺元素对于加法运算为0，于是$\sigma(0)=0$。现在设$\sigma(1)=l\in\mathbb{Z}$，则

$$\sigma(2)=\sigma(1+1)=\sigma(1)+\sigma(1)=l+l=2l,$$

由此可归纳证明：对每个正整数n，

$$\sigma(n)=ln。$$

因为

$$0=\sigma(n-n)=\sigma(n)+\sigma(-n),$$

从而

$$\sigma(-n)=-\sigma(n)=-ln,$$

这就表明σ的像集合为

$$\mathrm{Im}(\sigma)=\sigma(\mathbb{Z})=l\mathbb{Z}。$$

由于σ是自同构，$\mathrm{Im}(\sigma)$应当为$\mathbb{Z}$，即$\mathbb{Z}=l\mathbb{Z}$，所以必然$l=1$或$l=-1$。当$l=1$时，σ为恒等自同构I；当$l=-1$时，对每个$n\in\mathbb{Z}$，$\sigma(n)=-n$。容易验证这是整数加法群的自同构，所以$(\mathbb{Z},+)$共有两个自同构，即$\mathrm{Aut}(\mathbb{Z},+)=\{I,\sigma\}$是二阶(循环)群，其中$\sigma$定义为$\sigma(n)=-n$(对每个$n\in\mathbb{Z}$)，而$\sigma^2=I$。

再考虑有理数加法群$(\mathbb{Q},+)$。同样地，对加法群$\mathbb{Q}$的每个自同构σ，$\sigma(0)=0$，所以$\sigma(1)=\alpha$是非零有理数，与前同样地可知，对每个整数n，$\sigma(n)=n\alpha$。现在对有理数$\beta=\dfrac{n}{m}(m,n\in\mathbb{Z},m\geqslant 1)$，则

$$m\sigma(\beta)=\underbrace{\sigma(\beta)+\cdots+\sigma(\beta)}_{m\text{个}}=\sigma\underbrace{(\beta+\cdots+\beta)}_{m\text{个}}$$

$$= \sigma(m\beta) = \sigma(n) = n\alpha,$$

所以 $\sigma(\beta)=\frac{n}{m}\alpha=\beta\alpha$。然后验证映射

$$\sigma:\mathbb{Q}\to\mathbb{Q},\quad \sigma(\beta)=\beta\alpha(\text{对每个}\beta\in\mathbb{Q}),$$

满足 $\sigma(\beta_1\pm\beta_2)=\sigma(\beta_1)\pm\sigma(\beta_2)$，从而 σ 是加法群的自同态。当 $\alpha\neq0$ 时，$\mathrm{Im}(\sigma)=\alpha\mathbb{Q}=\mathbb{Q}$，从而 σ 为满同态。又对于 $\beta\in\mathbb{Q}$，

$$\beta\in\ker(\sigma)\Leftrightarrow\sigma(\beta)=\beta\alpha=0$$
$$\Leftrightarrow\beta=0(\text{因为}\alpha\neq0),$$

从而 $\ker(\sigma)=\{0\}$，即 σ 是单同态，因此 σ 为$(\mathbb{Q},+)$的自同构，我们把这个自同构记成 σ_α。

当 α 和 α'是不同的非零有理数时，σ_α 和 $\sigma_{\alpha'}$是不同的自同构，因为 $\sigma_\alpha(1)=\alpha$ 和 $\sigma_{\alpha'}(1)=\alpha'$是不同的，所以我们决定了

$$\mathrm{Aut}(\mathbb{Q},+)=\{\sigma_\alpha\mid\alpha\in\mathbb{Q}^*=\mathbb{Q}-\{0\}\}。$$

不少学生认为事情已经做完，这是一个适宜的地方，提醒同学，我们是在做群论，而不只是做集合论。以上我们只是决定了 $\mathrm{Aut}(\mathbb{Q})$ 这个集合，习题要求决定自同构群，我们还不知道 $\mathrm{Aut}(\mathbb{Q})$的群结构，要弄清自同构之间的群运算规律。对于 $\mathrm{Aut}(\mathbb{Q})$中两个自同构 σ_α 和 $\sigma_\beta(\alpha,\beta\in\mathbb{Q}^*)$，$\sigma_\alpha\sigma_\beta$ 在任意有理数 γ 上的作用为

$$(\sigma_\alpha\sigma_\beta)(\gamma)=\sigma_\alpha(\sigma_\beta(\gamma))=\sigma_\alpha(\gamma\beta)=\gamma\beta\alpha$$
$$=\sigma_{\beta\alpha}(\gamma)=\sigma_{\alpha\beta}(\gamma),$$

从而 $\sigma_\alpha\sigma_\beta=\sigma_{\alpha\beta}$，所以自同构的相乘对应于下标的实数乘法。于是考虑群 $\mathrm{Aut}(\mathbb{Q})$到非零有理数乘法群的映射

$$\varphi:\mathrm{Aut}(\mathbb{Q},+)=\{\sigma_\alpha\mid\alpha\in\mathbb{Q}^*\}\to(\mathbb{Q}^*,\times),\quad \sigma_\alpha\mapsto\alpha,$$

由上述可知 φ 是群的同态，并且 φ 是一一映射，所以 $\mathrm{Aut}(\mathbb{Q},+)$同构于非零有理数乘法群$\mathbb{Q}^*$：$\mathrm{Aut}(\mathbb{Q},+)\cong(\mathbb{Q}^*,\times)$。

最后我们决定 n 元循环群 G 的自同构群。由于 n 元循环群同构于$(Z_n=\mathbb{Z}/n\mathbb{Z},+)$，我们不妨设 $G=Z_n$。设 σ 是加法群 Z_n 的一个自同构，则 $\sigma(\bar0)=\bar0$，设 $\sigma(\bar1)=\bar a$(这里$\bar a$表示整数 a 模 n 的同余类)，由于 $\bar1$ 是加法群 Z_n 中的 n 阶元素，从而同构映射的像 $\sigma(\bar1)=\bar a$也应当是 Z_n 中的 n 阶元素。何时$\bar a$的阶为 n？

在这里，对于任意群 G（运算表示为乘法）和 G 中一个有限阶元素 g，同学应当由 g 的阶能够决定 g^l 的阶，其中 $l\in\mathbb{Z}$。

这本质上是初等数论。设 g 的阶为正整数 n，由带余除法可知，对每个整数 m，$g^m=1$（1 为 G 中幺元素）当且仅当 $n\mid m$（即 m 被 n 整除，或者说 m 是 n 的倍数）。现在我们决定 g^l 的阶，对每个 $m\in\mathbb{Z}$，有

$$(g^l)^m=1\Leftrightarrow g^{lm}=1\Leftrightarrow n\mid lm$$

$$\Leftrightarrow\frac{n}{(n,l)}\Big|\frac{l}{(n,l)}m\quad\text{（这里}(n,l)\text{表示 }n\text{ 和 }l\text{ 的最大公因子）}$$

$$\Leftrightarrow\frac{n}{(n,l)}\Big|m\quad\text{（由于}\frac{n}{(n,l)}\text{ 和}\frac{l}{(n,l)}\text{ 互素，即它们的最大公因子为 1），}$$

g^l 的阶是满足 $(g^l)^m=1$ 的最小正整数 m，也就是满足 $\frac{n}{(n,l)}\Big|m$ 的最小正整数 m，这显然得到 $m=\frac{n}{(n,l)}$，所以：

若 g 的阶为 n，则对每个 $l\in\mathbb{Z}$，g^l 的阶为 $\frac{n}{(n,l)}$。

回到原来的问题，在加法群 Z_n 中，$\bar{1}$ 的阶为 n，从而 $\bar{a}=a\bar{1}$ 的阶为 $\frac{n}{(n,a)}$。所以

$$\bar{a}\text{ 的阶为 }n\Leftrightarrow\frac{n}{(n,a)}=n\Leftrightarrow(n,a)=1\quad\text{（即 }a\text{ 与 }n\text{ 互素）。}$$

这就表明：若 σ 是加法群 Z_n 的自同构，则 $\sigma(\bar{1})=\bar{a}$，其中 a 是与 n 互素的整数。由初等数论知道，Z_n 看成是乘法半群时，$\bar{a}$ 是乘法可逆元（即存在 $b\in\mathbb{Z}$，使得 $\bar{a}\bar{b}=\bar{1}$，这相当于同余式 $ab\equiv1(\mathrm{mod}\ n)$），当且仅当 $(a,n)=1$。所以对加法群 $(Z_n,+)$ 的每个自同构 σ，$\sigma(\bar{1})=\bar{a}\in Z_n^*$，这里

$$Z_n^*=\{\bar{a}\in Z_n\mid(a,n)=1\}$$

是 Z_n 的所有乘法可逆元组成的乘法群，Z_n^* 的阶为 $\varphi(n)$。若 $\sigma(\bar{1})=\bar{a}(\bar{a}\in Z_n^*)$，则由同构性质可知

$$\sigma(\bar{i})=i\sigma(\bar{1})=i\bar{a}=\overline{ia}\quad(0\leqslant i\leqslant n-1),$$

直接验证由上式定义的 σ 是加法群的自同构，我们把它记成 σ_a。易知当 $a\equiv b(\mathrm{mod}\ n)$ 时，$\sigma_a=\sigma_b$，而不同的 $a\in Z_n^*$ 给出不同的自同构 σ_a，所以

$$\mathrm{Aut}(Z_n,+)=Z_n^*。$$

进一步考虑 σ_a 和 σ_b 的乘积（$a,b\in Z_n^*$），由于

$$\sigma_a\sigma_b(\bar{i})=\sigma_a(\overline{bi})=\overline{abi}=\sigma_{ab}(\bar{i})\quad(0\leqslant i\leqslant n-1),$$

可知 $\sigma_a\sigma_b=\sigma_{ab}$。这就表明有群同构

$$\mathrm{Aut}(Z_n,+)\cong(Z_n^*,\times),$$

其中 σ_a 对应于 $\bar{a}\in Z_n^*$。