高某人的随笔

——抽象代数

高

2021 年 12 月 5 日

前言

开坑时间:2021.8.30, 兜兜转转还是回来学数学了

时间:2021.11.28, 第一章总算是写的差不多了, 已经过去了快两个月, 直到今天这门学科才有入门的意思. 反反复复不知道看了多少遍，但似乎只有静下心来看才有效果。

抽象代数，拓扑学和泛函分析在同一学期开真是个不明智的选择，但似乎孙七七也完成了一学期学完这些的壮举。

使用的书籍为丘维生的《抽象代数基础》，杨子胥的《近世代数》，蔡天新的《数论——从同余观点出发》，一直想加一点 Artin 的《代数》，但似乎是没时间了

”在我看来，数学书（包括论文）是最晦涩难懂的读物。将一本几百页的数学书从头到尾读一遍更是难上加难。翻开数学书，定义、公理扑面而来，定理、证明接踵而至。数学这种东西，一旦理解则非常简单明了，所以我读数学书的时候，一般都只看定理，努力去理解定理，然后自己独立思考数学证明。不过，大多数情况下都是百思不得其解，最终只好参考书中的证明。然而，有时候反复阅读证明过程也难解其意，这种情况下，我便会尝试在笔记本中抄写这些数学证明。在抄写过程中，我会发现证明中有些地方不尽如人意，于是转而寻求是否存在更好的证明方法。如果能顺利找到还好，若一时难以觅得，则多会陷入苦思，至无路可走、油尽灯枯才会作罢。按照这种方法，读至一章末尾，已是月余，开篇的内容则早被忘到九霄云外。没办法，只好折返回去从头来过。之后，我又注意到书中整个章节的排列顺序不甚合理。比如，我会考虑将定理七的证明置于定理三的证明之前的话，是否更加合适。于是我又开始撰写调整章节顺序的笔记。完成这项工作后，我才有真正掌握第一章的感觉，终于送了一口气，同时又因太耗费精力而心生烦忧。从时间上来说，想要真正理解一本几百页的数学书，几乎是一件不可能完成的任务。真希望有人告诉我，如何才能快速阅读数学书。”

Infty

2021 年 12 月 5 日

目录

第一章 群论

1.1 基本知识

集合, 映射, 笛卡尔积在此不作赘述.

定义 1.1.1. 代数运算 设 A, B 和 D 是任意三个非空的集合, 则映射:

$$f : A \times B \to D, (a, b) \mapsto f(a, b)$$

称 f 为从 $A \times B$ 到 D 的一个代数运算简而言之, 代数运算就是满足封闭性的映射.

定义 1.1.2. 关系 设 A, B 是两个非空集合,$A \times B$ 的子集 R 称为 A, B 间的一个二元关系, 当 $(a, b) \in R$, 称 a 与 b 具有关系 R, 记作 aRb, 特别地, 当 $A = B$ 时,A,B 间的一个二元关系称为 A 上的一个二元关系.

应该还有另外一个定义, 但我已经忘了, 举个例子理解就好

例 1.1.3. $A = \{1, 2\}, B = \{0, 1\}, A \times B = \{(1, 0), (1, 1), (2, 0), (2, 1)\}$, 定义一种关系 R,R 为 $A \times B$ 的某一个子集, 我就取这样一个子集吧 $R = \{(1, 0), (2, 0), (2, 1)\}$, 该集合称为一个关系, 这正是我们熟悉的大于关系,R 中每一个元素的第一个分量都大于第二个分量.

定义 1.1.4. 等价关系 设 R 是集合 A 上的一个二元关系, 若满足:

- 反身性: 即 $\forall a \in A$, 都有 aRa,

- 对称性: 即 $\forall a, b \in A$, 若有 aRb, 则有 bRa
- 传递性: 即 $a, b, c \in A$, 若有 aRb 且 bRc, 则有 aRc

则称 R 是集合 A 上的等价关系. 当 aRb 时, 称 a 与 b 等价.

这个定义的描述方式并不显然, 所有的等价关系作为子集构成集合 A 本身, 也就是说, 每个等价关系都对应了一个类别, 这些类别将集合分割. 集合 A 的一个等价关系决定 A 的一个分类.

最为常用的例子就是模 m 的剩余类.

1.2　一点点对数论的补充

给出一些定义和定理, 作为回顾不给出证明, 当然这些证明也不难

定义 1.2.1. 整除 设 a,$b \neq 0$ 是任意两个整数, 如果存在一个整数 q 使得等式 $a = bq$ 成立, 我们就说 b 整除 a 或 a 被 b 整除, 记作 $b \mid a$. 在这种情况下我们称 a 为 b 的倍数, 而把 b 叫做 a 的因数或因子. 如果不存在这样的 q, 我们就说 b 不整除 a, 或 a 不被 b 整除, 记为 $b \nmid a$

定理 1.2.2. 若 a 是 b 的倍数,b 是 c 的倍数, 则 a 是 c 的倍数

定理 1.2.3. 若 a,b 都是 c 的倍数, 则 $a + b, a - b$ 也是 c 的倍数

定理 1.2.4. 带余除法 若 a,b 是两个整数,$b > 0$, 则存在整数 q 和 r, 使得 $a = bq + r, 0 \leq rb$ 成立, 且这里的 q 和 r 是唯一的

定义 1.2.5. 素数 素数的正因子只有 *1* 和它本身

定义 1.2.6. 最大公因数 设 a,b 是任意两个整数, 如果 $d \mid a, d \mid b$, 则称 d 是 a 和 b 的一个公因数,a 和 b 的公因数中最大的一个叫做 a,b 的最大公因数, 记为 *(a,b)*

定理 1.2.7. 若 a,b 是任意两个不全为 *0* 的整数, 则存在两个整数 s,t 使得 $as+bt=(a,b)$

定理 1.2.8. 设 a,b 时候任意两个不全为 *0* 的整数. 若 m 是任意正整数, 则:

$$(am,bm)=m(a,b)$$

若 d 是 a,b 的任意公因数, 则:

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

进而我们有 $(\frac{a}{(a,b)},\frac{b}{(a,b)})=1$

引理 1.2.9. 设 a,b,c 是三个整数,$(a,c)=1$, 则 ab,c 与 b,c 有相同的公因数; 若 b,c 不全为零, 则 $(ab,c)=(b,c)$

引理 1.2.10. 若 $c\mid ab$ 且 $(a,c)=1$, 则 $c\mid b$

定理 1.2.11. p 为素数的充分必要条件为 $p\mid ab$ 可推出 $p\mid a$ 或者 $p\mid b$

以下是我为了满足我强迫症加上去的内容, 事实上基本上没在书里遇到过

定义 1.2.12. 设 a,b 是任意两个非零正整数, 如果 $a\mid m,b\mid m$, 则称 m 是 a 和 b 的一个公倍数.a 和 b 的公倍数中的最小正数叫做 a,b 的最小公倍数, 记为 $[a,b]$

定理 1.2.13. 设 a,b 是任意两个正整数, 则 a,b 的所有公倍数就是 $[a,b]$ 的所有倍数, 且 $[a,b]=\frac{ab}{(a,b)}$

推论 1.2.14. 若 c 是 a,b 的公倍数,$(a,b)=1$, 则 $ab\mid c$

1.3　群的基本性质

定义 1.3.1. *群* 设 G 是一个非空集合, 如果满足下列 4 个条件:

- 在 G 中定义了一个代数运算 ”$\circ$”, 即满足封闭性,$\forall a,b\in G$, 有 $a\circ b\in G$
- 运算满足结合律:$\forall a,b,c\in G$, 有 $(a\circ b)\circ c=a\circ(b\circ c)$
- 存在 $e\in G$, 使得 $a\circ e=e\circ a=a,\forall a\in G$
- 对每一个 $a\in G$, 都存在 $b\in G$, 使得 $a\circ b=b\circ a=e$

则称 $(G,\circ)$ 是一个群, 简记 G.

如果一个群满足交换律, 我们称其为 abel 群.

定义 1.3.2. *半群和幺半群* 如果 G 只满足运算的封闭性和结合律, 则称 G 为半群, 如果半群 G 还含有单位元, 则称之为幺半群. 有时候单位元也称为幺元.

例 1.3.3. 群的单位元 e 是唯一的.

假设不唯一, 存在 $e,e_1,e\circ e_1=e=e_1\circ e$, 故单位元唯一.

例 1.3.4. 群中任意元素 a 的逆元是唯一的.

假设不唯一,b_1,b_2 为逆元, 存在 $b_1=b_1\circ e=b_1\circ(a\circ b_2)$
由结合律原式等于 $(b_1\circ a)\circ b_2=e\circ b_2$
由单位元得到 $e\circ b_2=b_2$
也就是 $b_1=b_2$

例 1.3.5. 群中的运算满足左右消去律.

例 1.3.6. 群 G 中,$(ab)^{-1}=b^{-1}a^{-1},(a_1a_2\cdots,a_n)^{-1}=a_n^{-1}\cdots a_2^{-1}a_1^{-1}$

由结合律及单位元,$(ab)\circ(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$

进而由数学归纳法可以证明 n 个的情况.

定义 1.3.7. 设 G 是群,$n \in \mathbb{Z}^{+}, \forall a \in G$ 规定 $a^n = a \cdot a \cdots a, a^0 = e, a^{-n} = (a^{-1})^n$

定义 1.3.8. 设 G 是加法群,$n \in Z^{+}, \forall a \in G$ 规定:$na = a + \cdots + a, 0a = 0, (-n)a = n(-a)$

例 1.3.9. 整数集 Z 对加法构成群

例 1.3.10. 设 $n \in Z^{+}, U_n = \{z|z^n = 1, z \in C\}$ 按复数乘法构成群

定义 1.3.11. 阶 群 G 的阶数为群 G 众元素的个数,G 的阶数为 n, 记为 $|G| = n$

1.4 循环群

有一种群是我们已经完全研究清楚的群, 这类群被称为循环群

定义 1.4.1. 循环群 设 G 是一个群, 如果 G 的每一个元素都能写出 G 中某个元素 a 的方幂 (乘法群) 或倍数 (加法群), 则称 G 为循环群. 这个元素 a 称为 G 的生成元. 并记作 $G = < a >$

注解 1.4.2. *1.* n 次单位根群和整数加群都是循环群

2. 循环群一定是交换群

例 1.4.3. 模 m 剩余类加群, 其中一个生成元为 $\bar{1}$

例 1.4.4. 域 F 上的线性空间 V 对加法构成一个 $abel$ 群

例 1.4.5. 一般线性群 $GL_n(F)$, 特殊线性群 $SL_n(F)$

1.5　全变换群

全变换群是一类值得研究的群, 原因是几乎任何群的研究都可以类比到全变换群当中

定义 1.5.1. 全变换群 非空集合 Ω 到自身的所有双射组成的集合, 对于映射的乘法构成一类群, 称它为集合 Ω 的全变换群

定义 1.5.2. 置换 当 Ω 为有限集合时,Ω 到自身的一个双射叫做 Ω 的一个置换. 设 Ω 有 n 个元素, 这时 Ω 的置换称为 n 元置换, 并称此时的全变换群为 n 元对称群

定义 1.5.3. n 元对称群 S_n 的任意子群称为 n 元置换群

定义 1.5.4. 非空集合 Ω 的全变换群 S_Ω 的任一子群称为 Ω 的变换群

定义 1.5.5. 设 $\sigma(i_1)=i_2,\sigma(i_2)=i_3,\cdots,\sigma(i_{r-1})=i_r,\sigma(i_r)=i_1$ 并且保持其余的元素不变, 则称 σ 为 S_n 中的一个 $r-$ 轮换, 记作 $\sigma=(i_1i_2\cdots i_r)$

注解 1.5.6.

1. *1*-轮换表示的是恒等变换
2. *2*-轮换也被称为对换
3. 如果两个轮换之间没有公共元素, 则称它不相交

定理 1.5.7. 不相交的两个轮换的乘积是可交换的

定理 1.5.8. 任一个 n 元置换都能表示成一些两两不相交的轮换的乘积, 出去排列次序以外, 表示法唯一

定理 1.5.9. 每一个轮换都可以表示成一些对换的乘积 $(i_1i_2\cdots i_r)=(i_1i_r)(i_1i_{r-1})\cdots(i_1i_3)(i_1i_2)$

定理 1.5.10. 任一个 n 元置换都可以表示成一些对换的乘积, 且表示方式不唯一, 但其中对换个数的奇偶性不变.

定义 1.5.11. 一个 n 元置换 σ 称为偶 (奇) 置换当且仅当 σ 可以表示成偶 (奇) 数个对换的乘积

注解 1.5.12.

1. 1-轮换 (恒等变换) 是偶置换, 可以看做 0 个对换
2. 2-轮换 (1 个对换) 是奇置换.

定理 1.5.13. r-轮换是偶 (奇) 置换, 当且仅当 r 是奇 (偶) 数

定义 1.5.14. 所有 n 元偶置换组成的集合, 按照映射的乘法成一个群, 称它为 n 元交错群, 记为 A_n

定理 1.5.15. S_n 中, 奇偶置换各半

1.6 子群

定义 1.6.1. 群 G 的非空集合 H 如果对于 G 的运算也成一个群, 则称 H 为 G 的子群, 记作 $H < G$

定义 1.6.2.

1. 仅有一个元素即单位元 e 组成的子集 $\{e\}$ 是 G 的一个子群
2. G 本身也是 G 的一个子群
3. $\{e\}$ 和 G 称为群 G 的平凡子群, 其余子群被称为非平凡子群

下面给出一个简单的定理, 该定理可由群的定义得到

定理 1.6.3. 设 G 是群,H<G, 则

1. $\forall a, b \in H \Rightarrow ab \in H$
2. H 的单位元就是 G 的单位元
3. $a \in H \Rightarrow a^{-1} \in H$

判断子群如果按照定义, 判断子集是否满足群定义的四条, 似乎太过繁琐了些, 下面定理给出了一些较为简单的判定

定理 1.6.4. *子群的判定* 设 H 是群 G 的非空集合, 则下列各条件等价

1. $H<G$

2. $\forall a, b \in H \Rightarrow ab \in H, a^{-1} \in H$

3. $\forall a, b \in H \Rightarrow ab^{-1} \in H$

以下定理是判断加法子群的最为常用且简单的方法

定理 1.6.5. *加法子群的判定* 设 H 是加法群 G 的非空集合, 则 $a, b \in H \Leftrightarrow a - b \in H$, 即对减法封闭

定理 1.6.6. 群 G 的任意个子群的交 $\bigcap_{i\in I} H_i$ 仍是 G 的子群.

定义 1.6.7. *生成子群* 生成子群 $<S>$ 是 G 中包含 S 的最小子群

定理 1.6.8. 设 S 是群 G 的一个非空子集, 则 $< S >= \{x_1^{m_1} x_2^{m_2} \cdots x_k^{m_k} | x_i \in S, m_i \in Z, 1 \leq i \leq k, k \in Z^+\}$

下列两个概念, 可类比代数中, 线性无关组和极大线性无关组的概念.

定义 1.6.9. *生成元集* 如果 $< S >= G$, 则称 S 的所有元素生成 G 或者说 S 是群 G 的一个生成元集

定义 1.6.10. *极小生成元集* 如果 $< S >= G$, 且任何 S 的真子集的生成子集都不是 G, 则称 S 是群 G 的极小生成元集

定义 1.6.11. *有限生成的群* 如果群 G 有一个生成元集是有限集, 则称 G 是有限生成的群

定义 1.6.12. 设 G 是群,$a \in G$

如果 $< a >$ 是无限群, 则称 a 是无限阶元, 记作 $|a| = \infty$

如果 $< a >$ 的阶为 n, 则称元素 a 的阶为 n, 记作 $|a| = n$, 则称元素 a 的阶为 n 记作 $|a| = n$

定理 1.6.13. 设 G 是群,$a \in G$, 则

1. $|a| = \infty \Leftrightarrow a^m \neq e, \forall m \in Z^+$
2. $|a| = n \Leftrightarrow n$ 是使得 $a^n = e$ 成立的最小正整数

注意, 不是只有循环群才有阶和元素的阶的概念, 任意群 G 以及任意群 G 中的元素都有.

注解 1.6.14. *在群 G 中, 单位元的阶为 1, 且只有单位元的阶为 1*

定理 1.6.15. 设 G 是群,$a \in G, |a| = n$ 则

1. $a^m = e \Leftrightarrow n|m$
2. $|a^k| = \frac{n}{(n,k)}, \forall k \in Z^+$

证明:

第一个必要性:

$a^m = e \Rightarrow n \mid m$, 作带余除法 $m = ln + r, 0 < r < n$, 只需证明 $r = 0$,$e = a^m = a^{ln+r} = (a^n)^l a^r = e^l a^r = a^r$

$a^r = e$, 而 $a^n = e, r < n$ 则矛盾. 故 r=0

充分性则显然, 直接代入即可.

第二个, 设 $|a^k| = s$

先证:$(a^k)^{\frac{n}{(n,k)}} = e$, 而 $(a^k)^{\frac{n}{(n,k)}} = a^{\frac{kn}{(n,k)}} = (a^n)^{\frac{k}{(n,k)}} = e^{\frac{k}{(n,k)}}$

显然 $\frac{k}{(n,k)}$ 是整数, 故所证成立, 因此 $s \mid \frac{n}{(n,k)}$

下面证明 $\frac{k}{(n,k)}$ 就是 a^k 的阶, 即 $\frac{n}{(n,k)} \mid s$

为了简便令 $n = n_1(n,k) = k_1(n,k)$, 有 $(n_1,k_1) = 1$, 这是因为 $(n,k) = ((n_1(n,k),k_1(n,k)) = (n,k)(n_1,k_1)$

等式两边消掉即得 $(n_1,k_1) = 1$

有 $(a^k)^s = (a^s)^k = e$ 因此 $n|ks \Rightarrow n_1(n,k)|k_1(n,k)s$ 从而 $n_1 \mid k_1 s$ 由于 $(n_1,k_1) = 1$, 因此 $n_1 \mid s$ 因此所证成立.

定理 1.6.16. 设 G 是群,$a,b \in G, |a| = n, |b| = m, ab = ba, (m,n) = 1$ 则 $|ab| = mn$

证明:

$a^n = e, b^m = e$

由于 $ab = ba$

$(ab)^{mn} = a^{mn}b^{mn} = (a^n)^m(b^m)^n = e$

因此 mn 至少是 ab 的阶的倍数, 设 $|ab| = s$

下面证明 $mn \mid s$

有 $e = (ab)^s n = a^{sn}b^{sn} = b^{sn}$ 因此 $m \mid sn$, 加之 $(m,n) = 1$ 因此 $m \mid s$, 同理 $n|s$

又因为 $(m,n) = 1$, 进而得到 $mn \mid s$

以上关于数论的定理均可以在数论补充那一节找到或简单推导而出

定义 1.6.17. *设 G 是群,A,B 是 G 的两个非空集合 $g \in G$, 规定 $AB = \{ab|a \in A, b \in B\}, \{g\}A = gA = \{ga|a \in A\}$*

设 H 是群 G 的子群,$a,b \in G$, 规定二元关系:$a\ b \Rightarrow b^{-1}a \in H$ 可以验证这是个等价关系

定义 1.6.18. *称 aH 是子群 H 的一个左陪集,a 为左陪集的一个代表*

注解 1.6.19.

1. *a 确定的等价类 $\bar{a}$ 就是以 a 为代表的左陪集*

2. *子群 H 本身也是一个左陪集,e 是它的一个代表, 这是因为 $H = eH$*

3. *群 G 中, 子群 H 的所有左陪集组成的集合就是群 G 的一个划分*

这些还是很直观的, 因此不给予证明

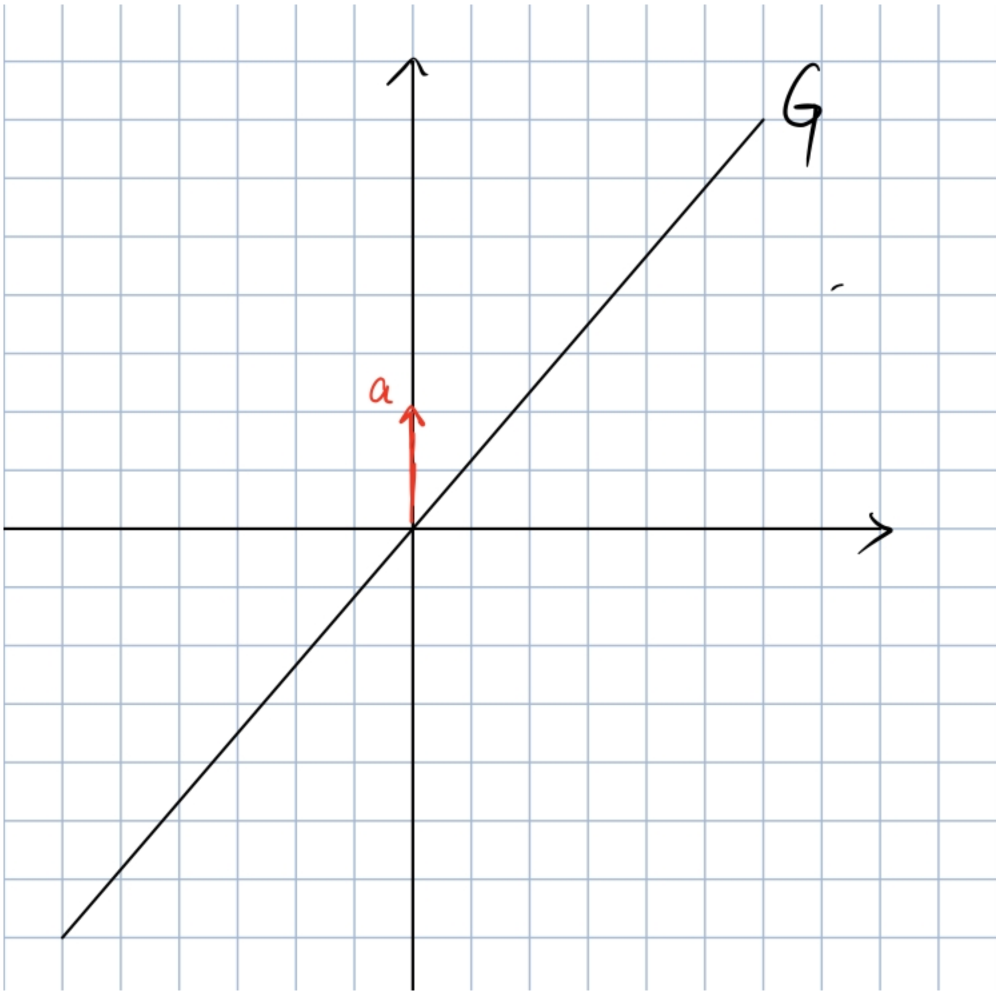
定义 1.6.20. *群 G 中, 子群 H 的所有左陪集组成的集合, 称为 G 关于子群 H 的左商集, 记作:*

$$(G/H)_i = \{aH|a \in G\}$$

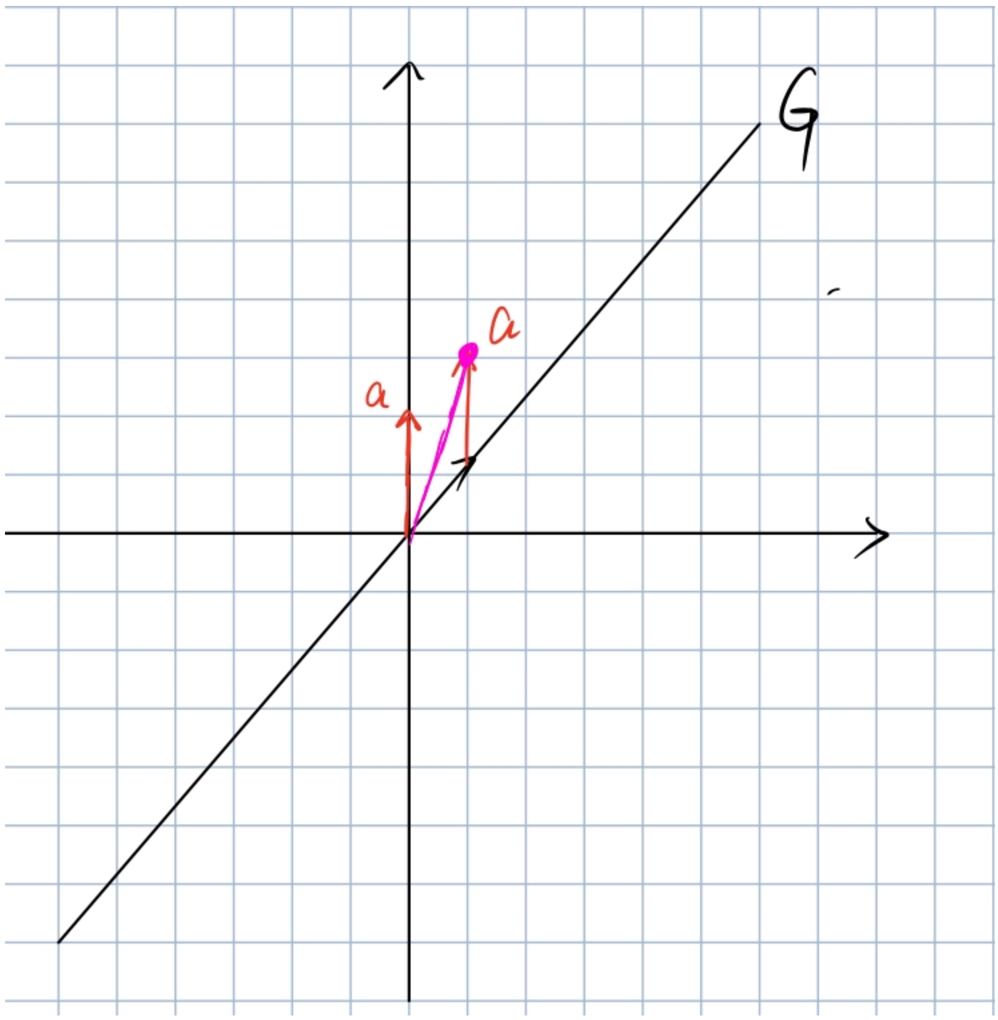
陪集和商集实际上是很自然的定义, 尽管看起来并不太自然, 实际上陪集在我们接触这个概念之前便有所接触, 比如对方程 $sins = 1$ 的解为 $\frac{\pi}{2} + 2k\pi$ 这就是陪集的形式, 有陪集的概念, 我们才把三角函数的解归类, 进而我们只需要研究一个周期的阶就行了, 这一个周期的阶也就是我们所说的代表元.

当然陪集还有更为直观的定义, 了解陪集的概念, 商集的引出则是自然的

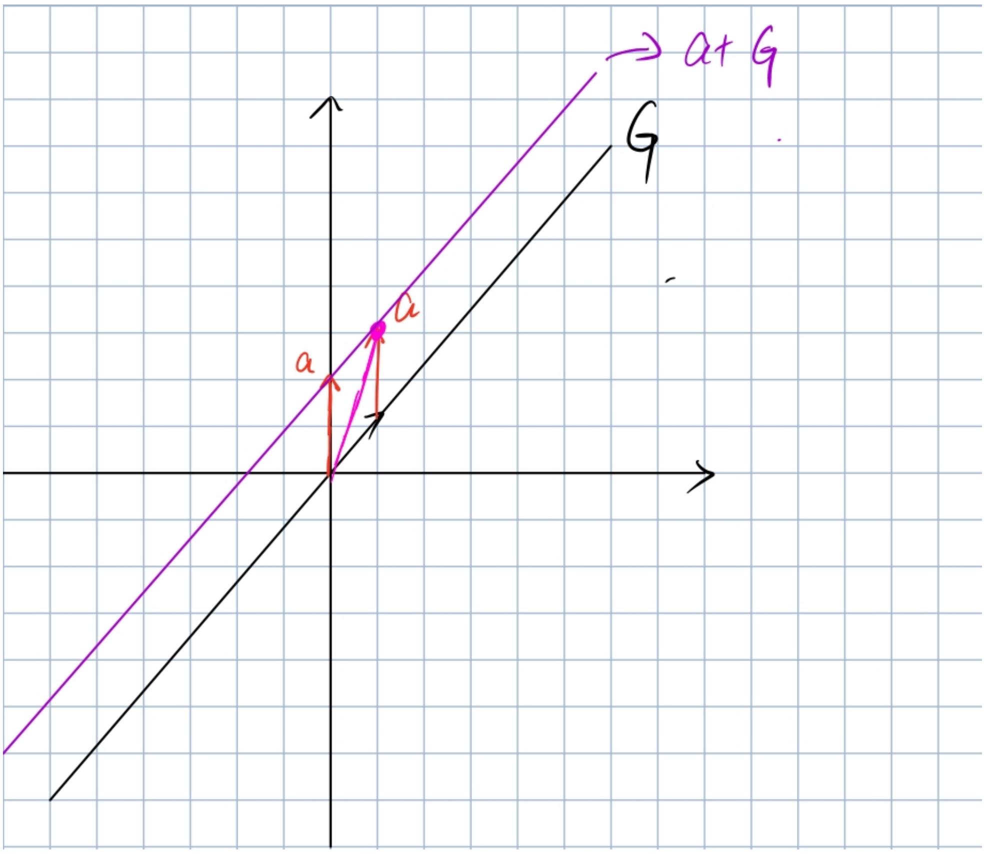
下图中 G 为子集,a 为任意一个向量



根据陪集的定义,$aG = a + G$, 取 G 中的一个元素, 也就是那条直线上的向量, 都会有这样紫色的一个向量生成



取遍 G 中的全部元素, 会生成一个陪集, 这个陪集和子群 G 平行.



在此基础上, 子群 G 的所有陪集的集合构成了商集.

商集天然的构成了空间的一个划分, 比如上图中会把二维欧氏平面划分成无数平行于子群 G 的直线.

推论 1.6.21. *1.* $aH = bH \Leftrightarrow b^{-1}a \in H \Leftrightarrow a^{-1}b \in H$

2. *子群 H 的任意两个左陪集要么相等, 要么不相交*

3. $aH = H \Leftrightarrow a \in H$

4. $b \in aH \Leftrightarrow aH = bH$

5. $G = \bigcup_{a\in G} aH$

右陪集和右商集可类似定义

定义 1.6.22. *群 G 关于子群 H 的左右商集的基数, 称为 H 在群 G 中的指数, 记作 [G:H]*

这个定义就是说, 商集把这个空间按子群 H 划分成了几个部分, 指数就是几

定理 1.6.23. *子群 H 与任一左陪集 aH 之间存在一一对应, 考虑映射:$\phi : h \to ah$*

该定理为显然的.

定理 1.6.24. *Lagrange 定理 有限群的任一子群 H 的阶必为群 G 的阶的因子, 即 $|G| = |H|[G : H]$*

$G = \sum\limits_{i=0}^{r-1} a_i H$

由于 H 与任一左陪集 aH 之间存在一一对应, 因此阶数相等 (书的编排问题, 真应该先讲群同构)

$|G| = \sum\limits_{i=0}^{r-1} |a_i H| = \sum\limits_{i=0}^{r-1} |H| = r|H|$

r 为陪集的个数, 证毕.

定理 1.6.25. *1. 有限群 G 的每一个元素的阶都是 G 的阶的因子, 若设 $|G| = m$, 则 $a^m = e, \forall a \in G$*

2. 素数阶群一定是循环群, 且每一个非单位元均为其生成元

3. 若 p 是素数, 且 a 不是 p 的倍数, 则 $a^{p-1} = 1(mod p)$

第二个结论, 素数阶群一定是循环群, 这似乎是个很神奇的结论, 按照结论一, 有限群 G 的每一个元素的阶都是 G 的阶的因子, 那么素数阶群的每个元素的阶都是 G 的阶的因子, 但由于素数的因子只有 1 和本身, 因此素数阶群除了单位元, 每一个元素的阶都是该素数, 也就是说可由一个生成元生成, 且每一个非单位元均为其生成元

定理 1.6.26. 1. 循环群的子群仍是循环群

2. 无限循环群的 $G =< a >$ 的全部子群为 $H_k =< a^k >, k = 0, 1, 2, \cdots$

3. 对 n 阶循环群 $G =< a >$ 的阶的每一个正因子, 都存在唯一的一个 s 阶子群, 他们构成 G 的全部子群

在之前循环群的时候说过, 循环群是已经完全研究清楚的群, 关于循环群的子群, 包括无限循环群和有限循环群, 也都可以轻易的找到.

定理 1.6.27. 设 G 是有限 $abel$ 群, 则 G 中存在一个元素, 它的阶是 G 中所有元素的阶的倍数.

定理 1.6.28. 设 G 为有限 $abel$ 群, 则 G 为循环群当且仅当对任意正整数 m, 方差 $x^m = e$ 在 G 中的解的个数不超过 m

定理 1.6.29. 有限域 F 的乘法群 F^* 是循环群

1.7 群同构

保持运算的双射, 被称为同构

定义 1.7.1. 设 $(G, \circ), (G', *)$ 是两个群, 如果存在双射 $\sigma : G \to G'$ 使得 $\sigma(a \circ b) = \sigma(a) * \sigma(b), \forall a, b \in G$ 称群 G 和 G' 是同构的, 记作 $G \cong G'$, 其中 σ 称为 G 到 G' 的一个同构映射

推论 1.7.2. 1. 同构的群, 基数必须相等, 也就是说, 阶相等

2. 同构的群由运算决定的性质必然相同, 如交换性, 结合律, 分配率

3. 同构关系是群之间的等价关系

推论 1.7.3. 设 $\sigma : G \in G'$ 为群同构, 则

1. $\sigma(e) = e'$

2. $\sigma(a^{-1}) = \sigma(a)^{-1}, \forall a \in G$

3. a 与 $\sigma(a)$ 同阶,$\forall a \in G$

4. $H < G \Rightarrow \sigma(H) < G'$

这是容易的性质, 所以嘛, 不证了

定理 1.7.4. 任意一个无限循环群都与 Z 同构

任意一个 m 阶循环群都与 Z_m 同构

1.8 群的直积

定义 1.8.1. 设 $(G, \circ), (G', *)$ 是两个群, 在笛卡尔积 $G \times G' = \{(g, g')|g \in G, g' \in G'\}$ 上, 定义运算: $(g_1, g_1')(g_2, g_2') = (g_1 \circ g_2, g_1' \circ g_2')$, 容易得到 $G \times G'$ 按上述运算构成一个群称为直积

其中单位元:(e, e'), 逆元 $(g, g')^{-1} = (g^{-1}, g'^{-1})$

注解 1.8.2. 1. 如果两个群的运算都是加法, 直积的运算也记成加法, 此时直积称为集合记作 $G \oplus G'$

2. 两个群都是有限群, 那直积也是有限群, 且 $|G \times G'| = |G| \cdot |G'|$

3. 两个群都是 $abel$ 群, 则直积也是 $abel$ 群

推论 1.8.3. 1. $G \times G' \cong G' \times G, \sigma : (g, g') \to (g', g)$

2. $G \times \{e'\} \cong G, \{e\} \times G' \cong G'$

定理 1.8.4. $Z_m \times Z_n \cong Z_{mn} \Leftrightarrow (m, n) = 1$

定理 1.8.5. 设 G 是群,$H < G, K < G$, 如果

1. $G = HK$

2. $H \cap K = \{e\}$

3. $hk = kh, \forall h \in H, k \in K$

则称 $G \cong H \times K$ 此时称 G 是子群 H 与 K 的内直积, 记作 $G = H \times K$

定理 1.8.6. 当群的运算为加法时, 内直积也称为内直和, 记作 $G = H \oplus K$ 设 G 是群,$H < G, K < G$, 如果

1. $G = H + K$

2. $H \cap K = \{0\}$

3. $h + k = k + h, \forall h \in H, k \in K$

则称 $G \cong H \times K$ 此时称 G 是子群 H 与 K 的内直积, 记作 $G = H \oplus K$

定理 1.8.7. 设 G 是加法群,$H_i < G(i = 1, 2, \cdots, s)$, 如果

1. $G = H_1 + H2 + \cdots + H_s = \sum\limits_{i=1}^{s} H_s$

2. $H_i \cap (\sum\limits_{j \neq i} H_j) = \{0\}$

3. $h_i + h_j = h_j + h_i, \forall h_i \in H, h_j \in H, \forall i \neq j$

则 $G = H_1 \oplus H_2 \oplus \cdots H_s$

1.9 群同态

定义 1.9.1. 设 $(G, \circ), (G', *)$ 是两个群, 如果存在映射 $\sigma : G \to G'$ 使得 $\sigma(a \circ b) = \sigma(a) * \sigma(b), \forall a, b \in G$ 其中 σ 称为 G 到 G' 的一个同态映射, 进一步, 若 σ 是单射, 称为单同态; 若满射, 则称为满同态.

定理 1.9.2. 设 $\sigma : G \to G'$ 为群同态, 则

1. $\sigma(e) = e'$

2. $\sigma(a^{-1}) = \sigma(a)^{-1}, \forall a \in G$

3. $H < G \Rightarrow \sigma(H) < G'$

4. 同态像 $Im(G) = \sigma(G) < G'$

定义 1.9.3. 设 $\sigma : G \to G'$ 为群同态, 定义
$ker\sigma = \{a \in G | \sigma(a) = e'\} = \sigma^{-1}(e')$

推论 1.9.4. 1. $ker\sigma < G$

2. σ 是单同态 $\Leftrightarrow ker\sigma = \{e\}$

3. σ 是满同态 $\Leftrightarrow Im\sigma = G'$

引出正规子群的概念, 正规子群就是让左陪集和右陪集相等的子群, 也就是 $aH = Ha$, 显然在 abel 群中, 任何子群都满足这样的性质, 但由于一般群并不一定满足交换律, 因此需要找到类似 abel 群子群相同功能的子群, 称之为正规子群.

有了这样的子群, 就可以引出商群的概念,

定义 1.9.5. 设 G 是群,$N < G$, 如果 $gH = Hg, \forall g \in G$, 则称 N 是 G 的正规子群, 记作 $N \lhd G$ 的正规子群, 记作 $N \lhd G$, 特别的,$abel$ 群的任一子群都是正规子群

定义 1.9.6. 平凡子群 $\{e\}$ 和 G 都是正规子群, 称它们为平凡的正规子群, 其他正规子群称为非平凡的

定理 1.9.7. 设 H 是群 G 的子群, 则下列条件等价:

1. $aH = Ha, \forall a \in G$

2. $aHa^{-1} \subset H, \forall a \in G$

3. $aha^{-1} \in H, \forall a \in G, h \in H$

4. $aHa^{-1} = H, \forall a \in G$

定义 1.9.8. 共轭子群 设 G 是群,$H < G$ 则对 $\forall g \in G, gHg^{-1}$ 也是 G 的一个子群, 称之为 H 的一个共轭子群

推论 1.9.9. 1. 子群 H 是正规子群当且仅当它的所有共轭子群都等于 H 本身

2. 设群同态 $\sigma : G \to G'$, 则 $ker\sigma$ 是 G 的正规子群

定义 1.9.10. 设 N 是 G 的正规子群, 则 $(G/N)_j = (G/N)_r = \{aN|a \in G\} \triangleq G/N$ 称为商集

定理 1.9.11. 商集 G/N 关于子集的乘法成一个群, 称为商群

定理 1.9.12. 1. G 为有限群 $|G/N| = \frac{|G|}{|N|}$, 这其实就是 *lagrange* 定理

2. 设 H<G, 则其两个左陪集的乘积仍是左陪集, 则 H 一定是正规子群

定理 1.9.13. 自然同态 设 N 是群 G 的一个正规子群, 令 $\pi : G \to G/N, a \to aN$ 则 π 是群 G 到商群 G/N 的一个满同态, 且 $ker\pi = N$

定理 1.9.14. 1. 上述的同态 π 称为自然同态或标准同态

2. 正规子群 N 是自然同态 π 的核

3. 商群 G/N 是群 G 在自然同态 π 下的像

定理 1.9.15. 群同态基本定理 设 σ 是群 G 到 G' 的一个同态, 则 $G/ker\sigma \cong Im\sigma$

这定理很直观, 按照核对空间进行划分得到商群和像集是同态的.

定理 1.9.16. 群第一同构定理 设 G 是群,$H < G, N \lhd G$, 则

1. $HN < G$

2. $H \cap N \lhd H$, 且 $H/(H \cap N) \cong HN/N$

定理 1.9.17. 设 G 是群,$H \lhd G, N \lhd G$ 且 $N \subset H$, 则

1. $H/N \lhd G/N$

2. $(G/N)/(H/N) \cong G/H$

我看不懂, 但似乎群同构定理似乎没有用到过

1.10 单群和可解群

定义 1.10.1. 如果群 G 只有平凡的正规子群, 则称 G 为单群

定理 1.10.2. $abel$ 群 G 是单群当且仅当 G 是素数阶循环群

定义 1.10.3. 群 G 中, 把 $xyx^{-1}y^{-1}$ 称为元素 x 与 y 的换位子 $xy = yx \Leftrightarrow xyx^{-1}y^{-1} = e$

定义 1.10.4. 群 G 中, 把所有换位子生成的子群, 称为群 G 的换位子群或导群, 记作 $[G, G]$ 或 G'

注解 1.10.5. 1. 所有换位子构成的集合不一定成群

2. 换位子群是所有换位子生成的子群

3. 类似的定义二次导群, 三次导群

定理 1.10.6. 群 G 是 $abel$ 群当且仅当 $G' = \{e\}$

定理 1.10.7. 群 G 的同态像 $Im\sigma$ 是 $abel$ 群当且仅当 $G' \subset ker\sigma$

定理 1.10.8. 设 G' 是 G 的导群,N 是 G 的正规子群, 则:

1. G/G' 是 *abel* 群

2. G/N 是 *abel* 群当且仅当 $G' \subset N$

注解 1.10.9. G 群 H 的所有 *abel* 商群中,G/G' 是最大的一个, 也就是所含元素最多的一个, 称之把 G'*abel* 化'

定义 1.10.10. 设 G 是导群, 有一个递降的子群列

$G \lhd G' \lhd G^{(2)} \lhd G^{(3)} \lhd \cdots$

称为群 G 的导群列

定义 1.10.11. 设 G 是群, 如果存在一个正整数 k, 使得有 $G^{(k)} = \{e\}$ 称为 G 的可解群; 否则, 称为不可解群.

1.11　群在集合上的作用

考虑全变换群, 每个群中的元素都是一种变化, 这个元素可以作用到另一个集合上, 使得集合做出一个变化.

群在集合上的作用因此而被抽象出来

定义 1.11.1. 设 G 是群,Ω 是非空集合, 如果存在 $G \times \Omega$ 到 Ω 的一个映射:$(a,x) \to a \circ x$ 满足

1. $(ab) \circ x = a \circ (b \circ \Omega), \forall a, b \in G, \forall x \in \Omega$

2. $e \circ x = x, \forall x \in \Omega, \forall x \in \Omega$

称为群 G 在集合 Ω 上有一个作用

定理 1.11.2. 设群 G 在集合 Ω 上有一个作用, 任意给定 $a \in G$, 令 $\varphi(a)x \triangleq a \circ x, \forall x \in \Omega$ 则 φ 是群 G 到 S_Ω(Ω 的全变换群) 的一个同态

证明同态相当于是证明:

$\varphi(ab)=\varphi(a)\varphi(b)$

即保持运算的性质, 然而 $\varphi(a)$ 实际上是一个映射, 要想证明左右相等, 需要证明左右两边作用到每一个元素上都相等.

即证明:$\forall x\in\Omega,\forall a,b\in G,\varphi(ab)(x)=(\varphi(a)\varphi(b))(x)$

$\varphi(ab)(x)=(ab)\circ x=a\circ(b\circ x)=\varphi(a)[\varphi(b)x]=[\varphi(a)\varphi(b)]x$

同态是容易的, 但是还需要验证 $\varphi(a)$ 到底是不是 S_Ω 中的元素, 也就是说, 这东西有没有逆映射存在.

因为证明了同态, 所以 $\varphi(a)\varphi(a^{-1})(x)=\varphi(aa^{-1})(x)=\varphi(e)(x)=e\circ x=x$

因此对于任意一个 $\varphi(a)$ 都存在一个逆映射 $\varphi(a^{-1})$, 因此它一定是全变换群中的元素.

该定理的逆命题也是成立的, 也就是说, 作用给出了一个从群 G 到集合 Ω 的全变换群的一个同态映射.

定义 1.11.3. *作用的核 作用的核为对应同态的核, 如果作用的核仅仅由单位元 e 组成, 称这个作用是忠实的.*

定义 1.11.4. *群在集合上的作用是忠实的, 是指相应的同态是单射*

例 1.11.5. *左平移 设 G 是一个群, 令 $G\times G\longrightarrow G,(a,x)\longrightarrow ax$*

定理 1.11.6. *Cayley 定理 任意一个群都同构于某一集合上的变换群*

Cayley 定理表明了研究变换群的重要性.

定理 1.11.7. *任意一个有限群都同构于一个置换群*

例 1.11.8. *共轭作用 $G\times G\to G,(a,x)\to axa^{-1}$*

定义 1.11.9. *令 $Z(G)=\{a\in G|ax=xa,\forall x\in G\}$ 称为群 G 的中心*

注解 1.11.10. *1. 群 G 在集合 G 上的共轭作用的核就是群 G 的中心*

2. $Z(G) \lhd G$

定义 1.11.11. 群 G 到自身的一个同构, 称为群 G 的一个自同构, 给定 $a \in G$, 形如 $\sigma_a(x) = axa^{-1}, \forall x \in G$ 的同构 σ_n 称为群 G 的一个内自同构.

定义 1.11.12. 群 G 的所有自同构组成的集合对于映射乘法成一个群, 称为 G 的自同构群, 记作 $Aut(G)$

群 G 的所有自同构组成的集合对于映射乘法成一个群, 称为 G 的自同构群, 记作 $Inn(G)$

定理 1.11.13. 1. $Inn(G) \triangleq Aut(G)$

2. $G/Z(G) \cong Inn(G)$

1.12 轨道与稳定子群

定义 1.12.1. 设群 G 在集合 Ω 上有一个作用, 对于 $x \in \Omega$, 令 $G(x) = \{g \circ x | g \in G\} \subset \Omega$ 称 $G(x)$ 是 x 的轨道

这实际上是陪集的推广.

定义 1.12.2. 设群 G 在集合 Ω 上有一个作用, 在集合 Ω 中规定二元关系:$x\ y \Leftrightarrow g \in G, s.t. y = g \circ x$, 上述二元关系是等价关系, 且一个等价类都是一个轨道

定义 1.12.3. 群 G 众,$a, b \in G$, 若存在 $g \in G$, 使得 $b = gag^{-1}$, 则称 b 与 a 共轭, 或称 b 是 a 的共轭元素.

注解 1.12.4. 1. 群中元素的共轭关系是等价关系, 每一个等价类称为一个共轭类:$\bar{x} = \{gxg^{-1} | g \in G\} \triangleq K_x$

2. 群 G 在集合 G 上的共轭作用的轨道就是共轭类

3. x 的共轭类只含有一个元素当且仅当 $x \in Z(G)$

4. $G = \bigcup K_x = Z(G) \bigcup\limits_{x \in Z(G)} K_x$

定义 1.12.5. 当 G 为有限群时,$|G| = |Z(G)| + \sum\limits_{x \in Z(G)} K_x$ 称之为有限群的类方程

定义 1.12.6. 设群 G 在集合 Ω 上有一个作用, 给定 $x \in \Omega$, 令 $G_x = \{g \in G | g \circ x = x\}$, 称之为 x 的稳定子, 稳定子是群 G 的子群称为稳定子群

定理 1.12.7. 设群 G 在集合 Ω 上有一个作用, 则对任意 $x \in \Omega$, 有 $|G(x)| = [G : G_x]$ 即 x 的轨道长等于 x 的稳定子群在 G 中的指数

如果有限群 G 在集合上有一个作用, 则每一条轨道的长是群 G 的因子, 即 $|G| = |G(x)||G_x|$

实际上, 这个和之前的商集的阶数与子群阶数的关系很像, 实际上陪集就是一个特殊的轨道.

以下是该定理的直观理解:

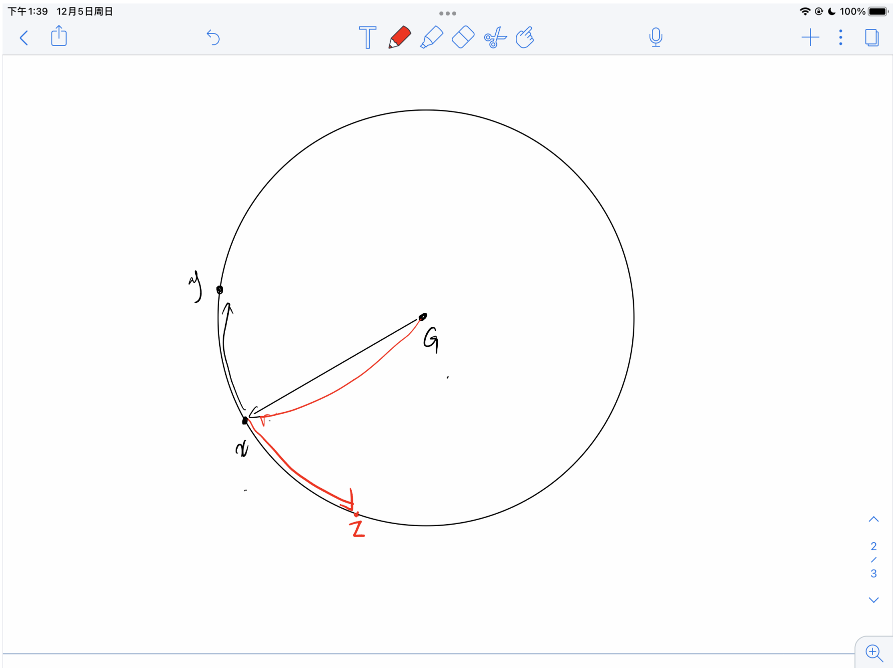
不妨先从代数上来看, 举出三元对称群的例子.

$$f1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} f2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} f3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$f4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} f5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} f6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

找一下元素 1 的轨道, 实际上经过三元对称群的作用,1 可以变换到 2, 也可以变换到 3. 因此在这个例子中, 只有一个轨道, 也就是 123 同轨. 再找 1 的稳定子, 分别是 f1 和 f2.$2 \times 3 = 6$ 也就是 3 元对称群的阶.

再从几何上来看一看:



如图这是一个轨道, 群 G 作用在 x 上, 黑色红色是群 G 中的元素作用在 x 上, 黑色将 x 作用到了 y, 红色将 x 作用到了 z, 将群 G 中所有元素都作用到 x 上, 就形成了如图这样的轨道, 轨道上的元素称之为同轨.

之后我们来找 G 中的元素, 是不是数一下轨道的阶数就行了呢? 不是, 因为一般的想总会存在这样的元素 $a, b, a \circ x = x, b \circ x = x$

也就是说, 有些点被重复的作用到了, 我们得把重复的也算上.

幸运的是, 对于将 x 作用到 x 上的元素, 我们称为稳定子, 那么将 x 作用到 y 的元素 $(a \circ x = y, b \circ x = y)$, 这类元素的个数和稳定子的个数是一样的

我们不妨假设稳定子群中所有的元素 $a_i, i = 1, 2, \cdots, n$ 且 $a_i \circ x = x$, 那么如果有 $b_1 \circ x = y$, 那么就有 $b_1 \circ a_i = y$, 因此对应会生成出 n 个 b_j, 使得 $b_j \circ x = y$,

相反的, 如果给定 $b_j \circ x = y, j = 1, 2, \cdots, m$, 就会有 $b_j^{-1} b_1 \circ x = x$, 因此 m=n.

因此, 我们要找到群 G 的阶数, 就是说找到轨道的阶数乘以稳定子的阶数即可.

完美!

注解 1.12.8. 考虑有限群 G 在自身上的共轭作用, 得 $|K_x| = [G : C_G(x)]$

定义 1.12.9. 设 G 是有限群, 若 $|G| = p^m$ 其中 p 为素数,$m \in Z^+$ 则称 G 为 p-群

定义 1.12.10. 设群 G 在集合 Ω 上有一个作用, 令 $\Omega_0 = \{x \in \Omega | g \circ x = x, \forall g \in G\}$, 称为群 G 的不动点群

定理 1.12.11. 设 $p-$ 群在有限集合 Ω 上有一个作用, 则 $|\Omega_0| \equiv |\Omega| (mod p)$

p-群必有非平凡的中心, 即不等于 $\{e\}$

1.13 Sylow 定理和有限 abel 群结构

这是什么东西, 这是什么东西! 我怎么一点也看不懂!!!

定理 1.13.1. *Sylow* 第一定理 (存在定理) 设 G 是群, 且 $|G| = n = p^l, (m,p) = 1, l > 0, p$ 为素数, 则对于任意 k,$1 \leq k \leq l$,G 中必有 p^k 阶子群

注解 1.13.2. 其中 p^l 阶子群称为群 G 的 *Sylowp−* 子群,*Sylow* p-子群的共轭子群也是 *Sylow* p-子群.

定理 1.13.3. *Sylow* 第二定理

1. G 的任一个 p^k 阶子群一定包含在某个 *Sylow* p-子群中

2. G 的任意两个 *Sylow* p-子群在 G 中共轭

3. 有限群 G 的 *Sylow* p-子群为正规子群当且仅当 G 的 *Sylow* p-子群的个数为 1

定理 1.13.4. *Sylow* 第三定理 G 的 *Sylow* p-子群的个数 r 满足 $r \equiv 1(modp), r|m$
$r = [G : N_G(P)], N_G(P)$ 为任一 *Sylow* p-子群 P 的正规化子

注解 1.13.5. *1.* 若 G 中有唯一的 s 阶子群 H, 则 H 必有正规子群

2. 若 $p/ |G|$,p 为素数, 则群 G 中必有 p 阶元

定理 1.13.6. 设 G 为有限群,$|G| = pq$, 其中 p,q 是两个不同的素数, 且 $p \nmid q-1, q \nmid p-1$, 则 G 为一个循环群

定理 1.13.7. 设 P 为 *abel* 群 p-群,$|P| = p'$, 则
$P \cong Z_{p^{k_1}} \times Z_{p^{k_2}} \times \cdots \times Z_{p^{k_r}}$
其中 $1 \leq k_1 \leq k_2 \leq \cdots \leq k_r, k_1 + k_2 + \cdots + k_r = l$

定理 1.13.8. 设 G 为 n 阶 *abel* 群,$n = p_1^{l_1} p_2^{l_2} \cdots p_s^{l_s}$, 其中 $p_1, p_2, \cdots, p_s$ 两两不同的素数,$l_i > 0, i = 1, 2, \cdots, s$, 则
$G \cong Z_{p^{k_{11}}} \times Z_{p^{k_{12}}} \times \cdots \times Z_{p^{k_r}}$

第二章 环论

2.1 环的基本概念

定义 2.1.1. 设 R 是一个非空集合, 并在 R 上定义了两个代数运算, 一个叫加法, 记作 $a+b$, 一个叫乘法, 记作 ab, 如果满足下列三个条件:

1. 对加法成一个 $abel$ 群
2. 对乘法满足结合律, 即 $\forall a, b, c \in G$ 有 $(ab)c = a(bc)$
3. 对乘法对加法的左右分配率:$\forall a, b, c \in G, a(b+c) = ab + ac, (b+c)a = ba + bc$

则称 $(R, +, \cdot)$ 是一个环, 简记 R

注解 2.1.2.

1. 环 R 对乘法不构成群
2. 若环对乘法还适合交换律, 则称为交换环
3. 设 R 是环, 若存在 $e \in R$, 使得 $ae = ea = a, \forall a \in R$, 则称 e 为环 R 的单位元, 此时 R 称为有单位元的环
4. 在有单位元 e 的环 R 中, 对于某个 $a \in R$ 如果存在 $b \in R$ 使得 $ab = ba = e$, 则称 a 为可逆元,b 称为 a 的逆元, 记为 a^{-1}
5. 对于环而言, 关于乘法不一定有单位元, 从而并不是所有元一定都可逆, 可逆元的逆元是唯一的

推论 2.1.3. 1. 环具有加法 $abel$ 群的所有性质

2. 由于环是加群, 从而可以定义倍数, 对于乘法, 只能定义正整数次幂

注解 2.1.4. 1. 交换环: 对乘法交换的环

2. 有单位元 1 的环: 存在乘法单位元的环

定义 2.1.5. 设 R 是环,$a, b \in R$ 且 $a \neq 0, b \neq 0$. 若 ab=0, 则称 a 为 R 的一个左零因子,b 为 R 的右零因子, 都简称为零因子.

注解 2.1.6. 1. 零因子一定不可逆, 可逆元一定不是零因子

2. 无零因子环: 没有 (非平凡) 零因子的环

3. 整环: 有单位元 1 的无零因子交换环

4. 除环: 非零元的全体对乘法构成群的环, 即 R 是有单位元 1 的环, 且每一个非零元都可逆

5. 域: 交换的除环

推论 2.1.7. 1. R 是无零因子环当且仅当若 $a \neq 0, b \neq 0$ 必有 $ab \neq 0$ 当且仅当从 $ab = 0$ 可以推出 $a = 0$ 或 $b = 0$

2. R 是无零因子环当且仅当左消去律成立

3. R 是无零因子环当且仅当右消去律成立

定义 2.1.8. 环的非空子集对于环的运算成一个环.R_1 是子环当且仅当 $a, b \in R_1 \Leftrightarrow a - b \in R_1, av \in R_1$ 即对减法和乘法封闭

2.2 理想

定义 2.2.1. 理想

1. $\forall a, b \in I \Rightarrow a - b \in I$ 即乘法封闭

2. $\forall a \in I, \forall r \in R \Rightarrow ra \in I, ar \in I$ 即吸收性

定理 2.2.2. 1. 生成理想 (S) 是环 R 中包含 S 的最小理想

2. 设 R 是有单位元的交换环,$\sigma_1, \sigma_2, \cdots, a_n \in R$, 则 $(a_1, a_2, \cdots, a_n) = \{r_1a_1 + r_2a_2 + \cdots r_na_n | r_i \in R, 1 \leq i \leq n\}$

3. 含有单位元 1 的理想必是整个环

定义 2.2.3. 设 A,B 是环 R 的两个非空子集合, 规定:

$$A + B = \{a + b\} | a_i \in A, b_i \in B, 1 \leq i \leq n, n \in Z^+$$

定理 2.2.4. 1. 设 IJ,K 是环 R 的两个理想, 则 I+J,IJ 都是环 R 的理想, 分布称为 I 与 J 的和与积, 且 $IJ \subseteq I \cap J \subseteq I + J$

2. 设 IJ,K 是环 R 的理想, 则以下规则成立:

   (a) I+J=J+I

   (b) (I+J)+K=I+(J+K)

   (c) (IJ)K =I(JK)

   (d) I(J+K)=IJ+IK

   (e) (J+K)I=JI+KI

3. 在整数环中,$m, n \in R$, 则,$(m, n) = 1 \Leftrightarrow (m)(n) = (m) \cap (n), (m, n) = 1 \Leftrightarrow (m) + (n) = (1) = Z$

定义 2.2.5. 设 R 是有单位元 *1* 的环,*IJ* 是 R 的理想, 如果 $I+J$=*R* 则称 I 与 J 互素

定理 2.2.6. *1.* 设 R 是有单位元 *1* 的环,*IJ*,*K* 都是 R 的理想, 如果 *IJ* 都与 K 互素, 则 *IJ* 业余 K 互素.

2. 设 R 是有单位元 *1* 的交换环,*IJ* 是 R 的理想, 则 *IJ* 互素可以推出 $IJ=I\cap J$

定义 2.2.7. 设 I 是 R 的理想, 则有加法商群 R/I 中定义乘法 $(r_1+I)(r_2+I)=r_1r_2+I$ 则 R/I 构成一个环, 称为 R 对 I 的商环或剩余类环

注解 2.2.8. *1.* 商环的元素 *r+I* 称为模 I 的剩余类

2. 若 R 是交换环, 则商环 R/I 也是交换环

3. 若 R 是有单位元 *1* 的环, 则商环 R/I 也是有单位元 *1+I* 的环

定义 2.2.9. 设 R 和 *R'* 是两个环, 如果存在映射 $\sigma: R\to R'$ 满足

1. $\sigma(a+b)=\sigma(a)+\sigma(b)$

2. $\sigma(ab)=\sigma(a)\sigma(b)$

3. $\sigma(1)=1'$ 对没有单位元的环不作要求

则称 σ 为一个环同态

进一步, 如果 σ 为单 *(满)* 射, 则称 σ 为一个单 *(满)* 环同态, 如果 σ 为双射, 则称 σ 为一个环同构, 此时记作 $R\cong R'$

定义 2.2.10. 设 σ 是环同态, 则 $\sigma^{-1}(0')=\{a\in R|\sigma(a)=0'\}$ 称为环同态 σ 的核, 记作 $ker\sigma$

定理 2.2.11. *1.* 设 σ 是环的满同态, 则必有 $\sigma(1)=1'$

2. σ 是单的环同态当且仅当 $ker\sigma = \{0\}$

3. σ 是满的环同态当且仅当 $Im\sigma = R'$

推论 2.2.12. 1. $\sigma(0) = 0', \sigma(-a) = -\sigma(a)$

2. 环同态像 $Im\sigma$ 是 R' 的子环

3. 环同态的核 $ker\sigma$ 是 R 的理想

定义 2.2.13. 设 I 是环 R 的理想, 则有商环 R/I, 进而有自然同态
$\pi : R \to R/I, r \to r + I$
其中 $ker\pi = I, Im\sigma = R/I$

定理 2.2.14. 环同态基本定理 设 $\sigma : R \to R'$ 是环同态, 则 $R/ker\sigma \cong Im\sigma$

定义 2.2.15. 设 $R_1, R_2, \cdots, R_s$ 都是环, 则有加法群的直和 $R_1 \oplus R_2 \oplus \cdots \oplus R_s$
其中加法运算为 $(a_1, \cdots, a_s) + (b_1, \cdots, b_s) = (a_1 + b_1, \cdots, a_s + b_s)$
再定义乘法运算 $(a_1, \cdots, a_s)(b_1, \cdots, b_s) = (a_1 b_1, \cdots, a_s b_s)$
称为环的直和

定义 2.2.16. 环的内直和 设 $I_1, I_2, \cdots, I_s$ 是环 R 的理想, 并且满足

1. $R = I_1 + I_2 + \cdots + I_s$

2. $I_i \cap \sum\limits_{j \neq i} I_j = \{0\}$

则 $R \cong I_1 \oplus I_2 \oplus \cdots \oplus I_s$

定义 2.2.17. 设 I 是环 R 的理想, 则 I 是环 r 的加法子群, 于是 $\forall a, b \in R$ 有 $a + I = b + I \Leftrightarrow a - b \in I$ 对于 $a, b \in R$ 如果 $a - b \in I$ 称 a,b 模 I 同余, 记作 $a \equiv b(modI)$

注解 2.2.18. 1. 模 I 同余关系是等价关系, 确定的等价类 $\bar{a} = a + I$ 即左陪集, 从而 R 对模 I 同余关系的商集就是商环 R/I

2. 若 $a \equiv b(modI), c \equiv d(modI)$, 则

   (a) $a + c \equiv b + d(modI)$

   (b) $ca \equiv cb(modI)$

   (c) $ca \equiv db(modI)$

定理 2.2.19. 设 R 是有单位元 1 的环, 它的理想 $I_1, I_2, \cdots, I_s$ 两两互素, 则 $R/(I_1 \cap I_2 \cap \cdots \cap I_s) \lhd R/I_1 \oplus R/I_2 \oplus \cdots \oplus R/I_s$

定理 2.2.20. 中国剩余定理 设 R 是有单位元 1 的环, 它的理想 $I_1, I_2, \cdots, I_s$ 两两互素, 则同余方程组

$$\begin{cases} x \equiv b_1(modI_1) \\ x \equiv b_2(modI_2) \\ \qquad \vdots \\ x \equiv b_s(modI_s) \end{cases}$$

2.3 素理想和极大理想

定义 2.3.1. 设 R 是有单位元 1 的交换环,P 是 R 的一个理想, 且 $P \neq R$, 如果从 $ab \in P$ 可以退出 $a \in P$ 或 $b \in P$, 则称 P 为 R 的一个素理想

定义 2.3.2. 设 R 是有单位元 1 的交换环, 则 R 的所有素理想组成的集合称为 R 的谱, 记作 $SpecR$

定理 2.3.3. 1. 整数环 Z 的每一个理想都是由一个非负整数生成的主理想

2. 域 F 上的一元多项式环 $F[x]$ 的每一个理想都是主理想, 其中非零理想可以由首项系数为 1 的多项式生成

3. 如果域 F 上的每一个次数大于零的一元多项式在 F 中都有根, 则称 F 是一个代数封闭域.(代数封闭域中的每一个不可约多项式都是一次多项式)

定理 2.3.4. 设 R 是有单位元 1 的交换环, 则 R 的理想 P 是素理想当且仅当商环 R/P 是整环 (整环是有单位元 1 的无零因子的交换环)

定理 2.3.5. 设 R 和 R 都是有单位元的交换环, 如果存在环的满同态 $\sigma : R \to R'$ 则:

1. $S' = \{R'\text{理想}\}$ 和 $S = \{R\text{的包含}ker\sigma\text{的理想}\}$ 存在双射

2. 对于 $I \in S$ 则有 $R/I \cong R'/\sigma(I)$

3. $SpecR'$ 与 $S_1 = \{R\text{包含}ker\sigma\text{的素理想}\}$ 存在双射

推论 2.3.6. 设 R 是环,I 是 R 的理想, 则

1. $S' = \{R/I\text{的理想}\}$ 与 $S = \{R\text{包含 } I \text{ 的理想}\}$ 存在双射

2. $S' = \{K/I|K \in S, \text{即 } R \text{ 中包含 } I \text{ 的理想}\}$

定义 2.3.7. 设 R 是环,M 是 R 的理想, 且 $M \neq R$, 如果 R 中包含 M 的理想只有 M 和 R, 则 M 称为 R 的一个极大理想

定理 2.3.8. 设 R 是有单位元 1 的交换环, 则 R 的理想 M 是极大理想当且仅当商环 R/P 是域

定理 2.3.9.
1. 设 R 是有单位元的交换环, 则 R 的极大理想一定是素理想, 反之不对

2. 设 R 是有单位元 1 的交换环, 则零理想是极大理想当且仅当 R 是域

3. 整数环中的理想 M 是极大理想当且仅当 M 由素数生成

4. 域 F 上的一元多项式 $F[x]$ 环中的理想 M 是极大理想当且仅当 M 由不可约多项式生成

2.4　有限域的构造

定义 2.4.1. 设 R,R' 都是有单位元的交换环, 如果存在单的环同态 $\sigma : R \to R'$ 则称 R 可以嵌入到 R', 此时也称 R' 是 R 的一个扩环, 并把 a 与 $\sigma(a)$ 等同, 记成 $a = \sigma(a)$

定理 2.4.2. 设 F_q 是含有 q 个元素的有限域, 其中 $q = p^r$,p 是素数, 如果 $m(x) = a_0 + a_1x + \cdots + a_nx^n \in F_q[x]$ 是 n 次不可约多项式, 则 $F_q[x]/(m(x))$ 是含有 q^n 个元素的有限域, 且它的每一个元素可唯一地表示成 $c_0 + c_1u + \cdots + c_{n-1}u^{n-1}$ 其中 $c_i \in F_q, 0 \leq i \leq n, u = x + (m(x)), u$ 满足 $m(u) = 0$

定义 2.4.3. 设 R 是有单位元 *1* 的交换环,R' 是 R 的扩环, 且 R' 是交换环, 任意取定 $u \in R'$, 我们把 R' 中包含 R 和 u 的所有子环的交, 称为 u 在 R 上生成的子环, 或 R 上添加 u 得到的子环, 记作 $R[u]$

$R[u]$ 是包含 R 和 u 的最小子环, 且 $R[u] = \{a_0 + a_1u + \cdots + a_nu^n | a_i \in R, 0 \leq i \leq n, n \in N\}$ 也称其为 u 在 R 上的多项式环

注解 2.4.4.
1. 代数数 t 的极小多项式存在且唯一
2. 代数数 t 的极小多项式一定在 Q 上不可约
3. 首 *1* 的以 t 为根的不可约有理多项式 *p(x)* 一定是 t 在 Q 上的极小多项式
4. 对于上述情形 *2*, 同态核是极小多项式生成, 即 $ker\sigma_t = (p(x))$, 其中 $p(x)$ 为 t 在 Q 上的极小多项式
5. 极小多项式的概念可以推广在任意一个域上

定义 2.4.5.
1. 有理数域 Q 上添加一个代数数得到的域 $Q[t]$ 称为代数数域, 记作 $Q(t)$

2. 如果复数 t 是某个首 1 的整系数多项式的根, 则复数 t 称为一个代数整数

3. n 次单位根群的生成元称为一个本源 n 次单位根

4. 有理数域 Q 上添加一个本源 n 次单位根得到的域称为第 n 个分圆域

定义 2.4.6. 设 p 是素数,$r \in Z^+$, 在环 $Z_{p^r}[x]$ 中, 如果首 1 的多项式 $f(x)$ 系数模 p 后得到的多项式 $\bar{f}(x)$ 在 $Z_p[x]$ 中不可约, 则称 $f(x)$ 在 $Z_{p^r}[x]$ 中基本不可约的

定义 2.4.7. 对于 m 次基本不可约多项式 $f(x) \in Z_{p^r}[x]$ 称其商环 $Z_{p^r}[x]/(f(x))$ 为一个 *Galois* 环.

它是含有 $(p^r)^m$ 个元素的有限环, 可以看成 Z_{p^r} 的扩环, 记作 $GR(p^r, m), GR((p^r)^m), R_{(p^r)^m}$

注解 2.4.8. 1. 整数环的分式域是有理数域

2. 任一整环的分式域存在, 且在同构的意义下唯一

3. 同构的整环, 其分式域也同构

以下讨论的环都是整环

定义 2.4.9. $a, b \in R$, 如果存在 $c \in R$ 使得 $a = bc$ 也称 b 整除 a, 记作 $b|a$, 此时称 b 是 a 的因子,a 是 b 的倍数

注解 2.4.10. 1. 可以以 *Q[x]* 为例理解

2. 环中的可逆元素本节统称为单位注意不一定是单位元

3. 整除关系具有反射性, 传递性, 但不具有对称性

4. $b|a \Leftrightarrow (b) \supseteq (a)$

5. $b|a_1, b|a_2 \to b|(r_1a_1 + r_2a_2), \forall r_1, r_2 \in R$

6. u 是 R 的单位当且仅当 $u|1$, 此时 $(u)=R$

7. 单位是任何元素 a 的因子, 任何元素都是单位的倍数, 这因为 $a=u(u^{-1}a)$ 单位的因子只能是单位, 这因为 $u=u_1u_2\to 1=u^{-1}u_1$

8. 零元 0 是任何元素 a 的倍数, 热呢 he 元素都是零元的因子, 这因为 $0=0a$, 但零元 0 的倍数只能是 0

定义 2.4.11. 如果 $a|b$, 且 $b|a$, 则称 a 与 b 相伴, 记作 $a\ b$

注解 2.4.12. 1. 相伴关系是等价关系

2. 相伴元互为因子和倍数, 即有相同的因子和倍数

3. $a\ b\Leftrightarrow (a)=(b)$

4. 零元 0 的相伴元只能是 0

5. 单位的相伴元只能是 0

6. 单位的相伴元只能是单位

7. $a\ b\Leftrightarrow \exists$ 单位 $u\in R, s.t. a=bu$ 即相伴元只能相差一个单位因子

8. $a\ b, c\ d\to ac\ bd$

定义 2.4.13. 如果 $b|a, a\nmid b$, 则称 b 是 a 的一个真因子

1. 真因子是因子但不是相伴元

2. 任何非零元 0 都是 0 的真因子

3. 单位没有真因子

定义 2.4.14. R 中任一单位以及 a 的相伴元, 统称为 a 的平凡因子, 其他因子称为非平凡因子

1. 非平凡因子一定是真因子

2. 单位没有非平凡因子

定义 2.4.15. 设 a 非 0 非单位, 如果 a 只有平凡因子, 则称 a 是不可约元, 否则, 称为可约元

1. 不可约元的因子只可能是单位或相伴元

2. 不可约元的相伴元只能是不可约元

3. 不可约元一定不可逆

定义 2.4.16. 设 a 非 0 非单位, 如果从 $a|bc$ 可以退出 $a|b$ 或 $a|c$, 则称 a 是一个素元.

定理 2.4.17. 1. 整环中, 素元一定是不可约元

2. 整环中,a 是素元当且仅当 (a) 为非零素理想

定理 2.4.18. 整环中,(a) 为非 0 极大理想, 则 a 为素元, 进而不可约