Jianting's Lecture Review Notes

近世代数
Contemporary Algebra

2020 Fall

Instructor：胡峻

Textbook：近世代数（2nd Ed.）韩士安、林磊

Review for Contemporary Algebra

Jianting Feng

14th November 2020

BEIJING INSTITUTE OF TECHNOLOGY

Contents

Chapter 1

群

1.1 群的概念

Definition 1.1.1 设 G 是一个非空集合，“$\cdot$” 是 G 上的一个代数运算，即对所偶的 $a, b \in G$，有 $a \cdot b \in G$. 如果 G 的运算还满足

1. $\forall a, b, c \in G$，有 $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
2. $\exists e$，$\forall a \in G$，有 $e \cdot a = a \cdot e = a$
3. $\forall a \in G$，$\exists b \in G$，使得 $a \cdot b = b \cdot a = e$

则称 G 关于运算 “$\cdot$” 构成一个**群**（*Group*），e 称为群 G 的**单位元**（*unit element*）或**恒等元**（*identity*），*3* 中的 b 称为 a 的**逆元**。容易证明单位元和逆元的唯一性。如果 G 的运算满足交换律，则称 G 为一个 ***Abelian* 群**。群 G 中的元素的个数称为 G 的**阶**（*Order*），记为 $|G|$，如果 $|G|$ 有限，则称 G 为**有限群**，否则称为**无限群**。

Example 1.1.1 整数集 $\mathbb{Z}$ 关于数的加法构成群，称为整数加群。

Example 1.1.2 全体非零有理数集合 $\mathbb{Q}^*$，关于数的乘法构成交换群。

Example 1.1.3 实数域 $\mathbb{R}$ 上的全体 n 阶方阵 $M_n(\mathbb{R})$ 关于矩阵的加法构成一个交换群。全体 n 阶可逆方阵 $GL_n(\mathbb{R})$ 关于矩阵的乘法构成非交换群。

Example 1.1.4 全体 n 次单位根组成的集合

$$U_n = \{x \in \mathbb{C} | x^n = 1\} = \{\cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n} | k = 0, 1, 2, \cdots, n-1\} \tag{1.1}$$

关于数的乘法构成一个 n 阶交换群。

Example 1.1.5 设 m 是大于 1 的正整数，则 $\mathbb{Z}_m$ 关于剩余类的加法构成群，这个群称为 $\mathbb{Z}$ 的**模 m 剩余类加群**。

Example 1.1.6 设 m 是大于 1 的正整数，记

$$U(m)=\{\bar{a}\in\mathbb{Z}_m|(a,)=1\}, \tag{1.2}$$

则 $U(m)$ 关于剩余类的乘法构成群。

Note 1.1.1 群 $(U(m),\cdot)$ 称为$\mathbb{Z}$ **的模** m **单位群**，这显然是一个交换群，当 p 为素数时，常记做 $\mathbb{Z}_m^*$，且 $|U(m)|=\phi(m)$，其中 ϕ 为 *Euler Totient* 函数。

Theorem 1.1.1 *1.* 群 G 的单位元与逆元唯一；

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

3. $\forall a,b\in G$，有 $(ab)^{-1}=b^{-1}a^{-1}$；

4. $\forall a,b,c\in G$，若 $ab=ac$ 或 $ba=ca$，则 $b=c$.

1.2 子群

Definition 1.2.1 设 G 是一个群，H 是 G 的一个非空子集。如果 H 关于 G 的运算也构成群，则称 H 为 G 的一个**子群**（*subgroup*），记做 $H<G$。

Example 1.2.1 对于任意群 G，G 本身以及只含有单位元 e 的子集 $H=\{e\}$ 是 G 的子群，称为 G 的**平凡子群**（*trivial subgroup*），其他的子群称为**非平凡子群**（*nontrivial subgroup*），群 G 不等于它自身的子群称为 G 的**真子群**（*proper subgroup*）.

Theorem 1.2.1 设 G 为群，$H<G$，则

1. 群 G 的单位元 e 是 H 的单位元；

2. 对于任意 $a\in H$，a 在 G 中的逆元就是 a 在 H 中的逆元。

Theorem 1.2.2 (子群的判别准则之一) 设 G 为群，H 是群 G 的**非空子集**，则 H 称为群 G 的子群的充分必要条件是

1. $\forall a,b\in H$，有 $ab\in H$；

2. $\forall a\in H$，有 $a^{-1}\in H$.

Theorem 1.2.3 (子群的判别准则之二（更为常用）) 设 G 为群，H 是群 G 的**非空子集**，则 H 称为群 G 的子群的充分必要条件是 $\forall a,b\in H$，有 $ab^{-1}\in H$.

Example 1.2.2 $SL_n(\mathbb{R})<GL_n(\mathbb{R})$（我们之后会证明，这其实是一个正规子群）。

Note 1.2.1 $GL_n(\mathbb{R})$ 称为**一般线性群**，$SL_n(\mathbb{R})$ 称为**特殊线性群**，这两个群在李代数（*Lie Algebra*）与微分几何（*Differential Geometry*）中有重要的意义。

Example 1.2.3 设 G 为群，记

$$C(G)=\{g\in G|gx=xg,\forall x\in G\} \tag{1.3}$$

则 $C(G) < G$，称为 G 的**中心**（*center*）.

Note 1.2.2 $C(G)$ 在后面关于有限群分类中有重要作用，详情参见 *Sylow* 定理与群的类方程（*class equation*。

Theorem 1.2.4 群 G 的任意两个子群的交集仍为 G 的子群（事实上，任意多个子群的交均为子群，但子群之并不一定是子群）。

Definition 1.2.2 定义

$$< a > := \{a^r | r \in \mathbb{Z}\} \tag{1.4}$$

是由一个元素 a 生成的群，称为**循环群**（*cyclic group*）。

Note 1.2.3 循环群在有限群的分类中也有重要作用，我们稍后会对此加以讨论。

1.3 群的同构

Definition 1.3.1 设 G 和 G' 是两个群，ϕ 是 G 到 G' 的**双射**（*bijection*），满足

$$\phi(a \cdot b) = \phi(a) \cdot \phi(b), \quad \forall a, b \in G, \tag{1.5}$$

则称 ϕ 为从群 G 到 G' 的一个**同构映射**（*homomorphism*），称群 G 与 G' **同构**（*isomorphism*），记做

$$\phi : G \cong G'$$

群 G 到自身的同构称为**自同构**（*automorphism*）。

一般地，证明两个群同构分为四步

1. 构造 G 到 G' 的对应关系 ϕ，并证明 ϕ 是一个映射（在商群中要证明 ϕ 是**良定义**（well-defined）的）；
2. 证明 ϕ 是单射，即 $\forall x, y \in G$，若 $\phi(x) = \phi(y)$，则一定有 $x = y$；
3. 证明 ϕ 是满射，即 $\forall x' \in G'$，存在 $x \in G$ 使得 $\phi(x) = x'$；
4. 证明 ϕ 保持运算，即 $\phi(x \cdot y) = \phi(x) \cdot \phi(y)$（注意区分群同构与环同构的差别）.

Theorem 1.3.1 (群同构的性质) 设 ϕ 是 G 到 G' 的同构映射，e 和 e' 分别是 G 与 G' 中的单位元，$a \in G$，则有

1. $\phi(e) = e'$；

2. $\phi(a^{-1}) = (\phi(a))-1$；

3. ϕ 是可逆映射，且 ϕ^{-1} 为 G' 到 G 的同构映射。

Corollary 1.3.1.1 设 $G \cong G'$，若 G 是 *Abelian* 群，则 G' 也是 *Abelian* 群；且 $|G| = |G'|$（若为有限群即为元素个数相同，若为无限群则为基数（*cardinal number*）相同）。

Theorem 1.3.2 *群的同构实际上在所有群构成的集合中定义了一个等价关系（equivalence relationship），即*

1. *（反身性）* $G \cong G$;
2. *（传递性）若* $G \cong G'$，$G' \cong G''$，*则* $G \cong G''$;
3. *（对称性）若* $G \cong G'$，*则* $G' \cong G$.

其中 G, G', G'' *都是群。*

Note 1.3.1 通过等价关系，实际上给出了所有群所在集合的一个划分，我们可以通过研究一小部分群搞清楚所有群的结构，这一点在有限群的分类中具有极其重要的意义。

设 X 是任意集合，令 S_X 是 X 的全体可逆变换构成的集合，定义两个可逆变换的合成

$$\begin{aligned} \tau \circ \sigma : \quad & X \to X, \\ & x \mapsto \tau(\sigma(x)), \quad \forall x \in X \end{aligned}$$

仍为 X 的可逆变换。于是 $\circ$ 是 S_X 的代数运算，容易验证 S_X 关于变换的合成构成群（满足群的四条性质）。

Theorem 1.3.3 (Cayley 定理) *每一个群都同构与一个变换群。*

设 G 是群，$a \in G$，定义 ϕ_a 如下

$$\phi_a(x) = ax, \quad x \in G$$

称 ϕ_a 为一个左乘变换（左平移），全体左乘变换的集合 $G_l = \{\phi_a | a \in G\}$，称为 G 的左正则表示（left regular representation）。容易证明 $G \cong G_l$。

Note 1.3.2 同理我们可以定义右平移与右正则表示，有完全相同的结论成立。