抽象代数笔记

rogeryoungh

2023 年 12 月 13 日

目录

第一章　初等数论

注意我们的理论基础是整数，尽量通过分类讨论的方式得到结论。而且也要把握脉络，抓住重点，不要迷失于无谓的细节中。

自然数 $\mathbb{N}$ 、正整数 $\mathbb{N}^+$ 和整数 $\mathbb{Z}$ 我们是熟知的。

1.1　整除

1.1.1　整数公理

整数的公理

我们熟知一些整数的代数算律

结合律：$(a+b)+c=(a+b)+c$。

交换律：$a+b=b+a$。

消去律：

定义 1.1.1

对于整数 a,b，其中 $a\neq 0$，若存在整数 c，它使得

$$b=ac$$

则 b 叫做 a 的倍数，a 叫做 b 的因数，记作 $a\mid b$。

有时也称作 a 能整除 b，或 b 能被 a 整除，或 a 能除尽 b，或 b 能被 a 除尽。

若 a 不能整除 b，我们就记作 $a\nmid b$。

引理 1.1.2

如果对于整数 a,b 满足 $a\mid b$，则有

$$(-a)\mid b,\quad a\mid(-b),\quad(-a)\mid(-b),\quad |a|\mid|b|$$

这个比较显然，由定义知存在 c 使得 $b=ac$，再构造验证即可。

引理 1.1.3

对于整数 a,b,c 有 $a\mid b,b\mid c$，则有 $a\mid c$。

证明　因为 $a\mid b,b\mid c$，故存在整数 d,e 使得 $b=ad,c=be$。

因此存在整数 $f=de$ 使得 $c=af=ade$，故 $a\mid c$。 □

引理 1.1.4

对于整数 a,b 有 $|a|\mid|b|$，若 $|a|<|b|$ 则有 $a=0$。

证明 因为 $|a|\mid|b|$，则存在整数 c 使得 $|a|=|b|c$。那么有

$$0\leqslant|a|=|b|c<|b|$$

即 $0\leqslant c<1$，又 c 为整数，故 $c=a=0$。 □

定理 1.1.5

对于整数 a,b，若 $b\neq0$ 则一定存在唯一一对 q,r 使得

$$a=bq+r,\quad 0\leqslant r<|b|$$

证明 先证明存在性。

(1) 若恰 $b\mid a$，则必存在 c 使得 $a=bc$，此时有 $q=c,r=0$。

(2) 否则一定存在 n 使得 $n|b|<a<(n+1)|b|$，即存在 $0<r<|b|$ 使得 $a=|b|n+r$。

当 $b>0$ 时，令 $q=n$；当 $b<0$ 时，令 $q=-n$ 则有

$$a=bq+r,\quad 0\leqslant r<|b|$$

再证明唯一性。设存在两对 q_1,r_1 和 q_2,r_2 使得

$$a=bq_1+r_1=bq_2+r_2,\quad 0\leqslant r_1,r_2<|b|$$

相减有

$$a-a=b(q_1-q_2)+r_1-r_2=0$$

即 $r_1-r_2=-b(q_1-q_2)$，因此有 $b\mid(r_1-r_2)$。而 $|r_1-r_2|<|b|$，又引理知有 $|r_1-r_2|=0$。故

$$r_1=r_2,q_1=r_2$$

即两对相同。 □

定义 1.1.6 ◇ 素数

设整数 $p\neq0,\pm1$，若它除了 $\pm1,\pm p$ 外没有其他的因数，则称 p 是素数；否则称 p 是合数。

我们讲到素数时，一般指正的。把素数的集合记作 $\mathbb{P}$。

定理 1.1.7

若 a 是合数，则必存在素数 p 使得 $p\mid a$。

此时称该素数为 a 的素因数。

定理 1.1.8

设整数 $a \geqslant 2$，那么 a 一定可以分解为素数的乘积，即

$$a = p_1 p_2 \cdots p_s$$

其中 $p_j \in \mathbb{P}$。

OI 中，经常会求符合命题 $P(k)$ 的数 k 有多少个，此时我们有记号 $[P(k)]$，当命题成立时其值为 1，命题为假时值为 0。

1.1.2 公因数与公倍数

定义 1.1.9 ⋄ 公因数

设 a_1, a_2 是两个整数，若 $d \mid a_1$ 且 $d \mid a_2$，则称 d 是 a_1, a_2 的公因数。一般的，若对于一组整数 $a_1, \cdots, a_k$，有 $d \mid a_i$，则称 d 是 $a_1, \cdots, a_k$ 的公因数。

把 a_1, a_2 的正的公因数中最大的，称作最大公因数，记作 (a_1, a_2) 或 $\gcd(a_1, a_2)$。

由定义易知，若 $(a_1, a_2) = d$，则 $(a_1/d, a_2/d) = 1$。

定义 1.1.10 ⋄ 互素

若 $(a_1, a_2) = 1$，则称 a_1, a_2 是互素的。

类似的，对于多个数也类似的有最大公因数和互素等概念。

定义 1.1.11 ⋄ 公倍数

设 a_1, a_2 是两个整数，多 $a_1 \mid l$ 且 $a_2 \mid l$，则称 l 是 a_1, a_2 的公倍数。一般的，若对于一组整数 $a_1, \cdots, a_k$，有 $a_j \mid l$，则称 l 是 $a_1, \cdots, a_k$ 的公倍数。

把 a_1, a_2 的正的公倍数中最小的，称作最小公因数，记作 $[a_1, a_2]$ 或 $\operatorname{lcm}(a_1, a_2)$。

由定义易知，对于 $m > 0$ 有 $[ma_1, ma_2] = m[a_1, a_2]$。

1.1.3 带余除法

定理 1.1.12

设整数 a, b 且 $a \neq 0$，则一定存在唯一的一对整数 q, r 使得

$$b = qa + r, 0 \leqslant r < |a|$$

更一般的，对于任意的 d 总存在一对 q, r 使得

$$b = qa + r, d \leqslant r < |a| + d$$

当 $d = 0$ 时，称 r 为最小非负余数，$d = 1$ 时称 r 为最小正余数。计算机一般是 $d = 0$。

引理 1.1.13

设 $a > 0$，则任意整数被 a 除后所得的最小非负余数只可能是 $0, \cdots, a-1$ 中的一个。

于是我们可以按余数对整数进行分类。

第二章　群

2.1　置换

为方便起见，本节简记集合 $\{1, \cdots, n\}$ 为 $\mathbb{N}_n^+$。

定义 2.1.1

设 X 是一个集合，则 X 中的一个表是指函数 $f: \mathbb{N}_n^+ \to X$。若 X 中的表 f 是双射，则称 f 为 X 的一个排列。

因此，X 的排列是 X 的所有元素组成的一个无重复的 n 元组。显然 n 元集恰有 n^n 个表和 $n!$ 个排列。

定义 2.1.2 ◇ 置换

设 X 是一个集合（可能是无限集），X 的一个置换是指双射 $\alpha: X \to X$。

给定一个有限集 X，$|X| = n$，设 $\phi: \mathbb{N}_n^+ \to X$ 是一个排列，若 $f: \mathbb{N}_n^+ \to X$ 是 X 的一个排列，则 $f \circ \phi^{-1}: X \to X$ 是 X 的一个置换。反之，若 $\alpha: X \to X$ 是 X 的一个置换，则 $\alpha \circ \phi: \mathbb{N}_n^+ \to X$ 是 X 的一个排列。

即排列和置换只是描述同一事物的两种不同方法，使用置换而不是排列，其好处是置换可做合成运算。

若 $X = \mathbb{N}_n^+$，则我们可以使用一个二行记号来表示置换 α：

$$\alpha = \begin{pmatrix} 1 & 2 & \cdots & j & \cdots & n \\ \alpha(1) & \alpha(2) & \cdots & \alpha(j) & \cdots & \alpha(n) \end{pmatrix}$$

其底行是排列 $\alpha(1), \alpha(2), \cdots, \alpha(n)$。

定义 2.1.3 ◇ 对称群

集合 X 的所有置换构成的族，记为 S_X，称为 X 上的对称群。当 $X = \mathbb{N}_n^+$ 时，S_X 通常记为 S_n，并称为 n 次对称群。

注意到，有些置换是交换的，有些置换又不是交换的。