

**定义 5-5.1** 如果群  $\langle G, * \rangle$  中的运算  $*$  是可交换的, 则称该群为阿贝尔群, 或称交换群。

**定义 5-5.2** 设  $\langle G, * \rangle$  为群, 若在  $G$  中存在一个元素  $a$ , 使得  $G$  中的任意元素都由  $a$  的幂组成, 则称该群为循环群, 元素  $a$  称为循环群  $G$  的生成元。