

研讨主题（4）抽象代数

说明：

研讨学习选题是开放的，不做强制性约束，同学们可以根据小组与个人情况拓展或调整研讨具体内容，并决定仅是初步了解还是深入研习，但每个成员对选题或相关内容有所初步了解与思考是必须也是重要的。

1 阿贝尔与伽罗瓦：传奇与思想

阿贝尔与伽罗瓦是数学史上的传奇，他们是天际间的流星，却留下了永恒的光芒。请你谈谈对他们的了解，可以是他们的人生故事或相关的言语，也可以是阿贝尔理论、伽罗瓦理论的思想、方法的提出过程以及你的理解与感想。如果查阅了资料，请勿直接拷贝，用自己的文字简要总结即可。

2 群、环、域：理论与在密码学中的应用

请总结群、环、域等相关理论，并探讨其在密码学中的应用（如RSA、椭圆曲线加密等），简要介绍方法或过程即可。

3 群码：基于群论的纠错码构建理论与实现

纠错码是提高计算机和数据通信系统可靠性的重要基础，本选题探讨基于群论的纠错码设计原理与编程实现。

4 同态与同构：思想与应用

同态、同构是抽象代数中重要的概念或思想，我们生活中也有很多同态或同构的例子和应用，你所学习的数学也有相当多的例子（如对数构成的同构映射、各种变换等），从计算机角度看，我们也需要有意识地构建和应用同态、同构，如算法设计、软件开发、同态加密等。请你就此展开一些讨论，可以介绍基本思想，可以举例（脑洞大开的例子也是可以的）。