数学と社会

2 単位 (選択) 3 年 (後期)

片山 真一 · 教授 / 総合理数学科, 大渕 朗 · 教授 / 総合理数学科

【授業目的】・代数的構造についての基礎及びその様々な場に於ける応用についての基礎に関する講義を行う. 講義では代数構造の代表的な分野である代数的整数論と代数幾何学の初歩とその応用である暗号理論, 符号理論の解説を行う. ・目標は群, 環に於ける準同型定理の理解, 有限体の定義の理解, 線形符号の定義とシングルトンの不等式の理解である (大渕). また公開鍵暗号系の仕組みと剰余類群の応用として, RSA 暗号系を理解 する (片山).

【授業概要】・代数的構造に関する基礎理論 (群・環・体及び整数論) についての基本的な知識及び応用 (符号理論・暗号理論) への理解が深まるように講義を行う. ・群論の初歩, 基礎的な環論及び体論を解説する. これを受けて線形符号に関する初歩的な一般論を講義する (大渕). また公開鍵暗号系に関する基礎理論を講義する (片山).

【キーワード】符号理論, 暗号理論, 現代代数学

【先行科目】『代数基礎 I』(1.0), 『代数基礎 II』(1.0)

【関連科目】『代数学 I』(0.5), 『代数学 II』(0.5)

【到達目標】代数的構造に関する基礎理論の理解と符号理論と 暗号理論への応用

【授業計画】

1. 群の定義
2. 準同型定理
3. 環の一般論
4. 準同型定理
5. 有限体概説
6. 符号の定義
7. 線形符号
8. シングルトンの不等式
9. 暗号の歴史
10. 対称鍵暗号系の仕組み
11. 計算困難性
12. 非対称鍵暗号系の仕組み
13. RSA 暗号系
14. デジタル署名の仕組み
15. RSA 署名およびまとめ
16. 総括授業

【成績評価】出席および提出レポートによる総合評価を行う.

【再試験】無

【教科書】特に指定しない.

【授業コンテンツ】http://cms.db.tokushima-u.ac.jp/cgi-bin/toURL?EID=220350

【連絡先】

⇒ 片山 (1304, 656-7228, katayama@ias.tokushima-u.ac.jp) Mail
⇒ 大渕 (088-656-7297, ohbuchi@ias.tokushima-u.ac.jp) Mail