離散数学

科目ナンバー　2B205
専門基礎　　選択　　2単位

渡辺　隆治

1. 授業の概要（ねらい）

情報数理の基礎である代数系、有限体、整数論についての入門レベルのコースです。
演算と代数系、半群と群、環と体、情報の伝達、符号の誤り、誤りの検出と訂正、有限体、ハミング符号、巡回符号、BCH符号、暗号、整数、素数と素因数分解、ユークリッドの互除法、1次不定方程式、合同式、フェルマーの小定理、RSA暗号について学習します。
サブテキストに書かれた単元ごとの学習の狙いに基づいてテキストを読み、各単元末の演習問題を解くことにより、その内容の理解を深め、運用能力の定着を図る授業です。
この科目は、情報科学科のディプロマポリシーの項目2に関連する科目です。

2. 授業の到達目標

群、環、体の基礎を理解する。
情報の誤りを検出・訂正する符号の仕組みの基礎を有限体に基づき理解する。
公開鍵暗号のひとつであるRSA暗号の仕組みの基礎を整数論に基づき理解する。

3. 成績評価の方法および基準

科目修得試験については、60点以上の得点を合格とします。
レポート課題の評価を4割、科目修得試験の成績を6割の割合で考慮して、成績評価をします。
レポートの添削によりフィードバックを行います。

4. 教科書・参考文献

教科書
寺田文行,中村直人,釈氏孝浩,松居辰則　　『情報数学の基礎』［第1章、第2章］
サイエンス社　（ISBN 4-7819-0914-0）
参考文献
小倉久和,高浜徹行　　『情報の論理数学入門』　近代科学社　（ISBN 9784764901803）

5. 準備学修の内容

予習として、サブテキストの学習の狙いと要点の確認を読み、概要を把握してからテキストの学習に進んで下さい。各単元末に演習問題が設けてあります。復習および次の回の授業の準備として必ず解答して下さい。各回の予習復習の時間がテキストの学習時間の概ね2倍程度となるように講義内容と演習問題を準備しています。
高等学校数学の『数学Ⅰ』の「数と式」、『数学A』の「整数の性質」、『数学Ⅱ』の「式と計算」と通信教育課程の「線形代数」の理解を前提としていますので、その内容を事前に確認しておいて下さい。

6. その他履修上の注意事項

各単元末の演習問題の計算過程を含む解答がレポート課題です。レポートは手書きで作成して下さい。
科目修得試験では、参考資料等の持ち込みを禁止します。
科目修得試験には、各単元末の演習問題またはその類似問題を出題します。
高等学校用教科書はhttp://www.mext.go.jp/a_menu/shotou/kyoukasho/mokuroku.htmより探せます。

7. 授業内容

【第1回】　代数系　：　演算と代数系、半群と群
【第2回】　代数系　：　置換群、巡回群
【第3回】　代数系　：　環と体
【第4回】　有限体と符号　：　情報の伝達、符号の誤り
【第5回】　有限体と符号　：　誤りの検出と訂正
【第6回】　有限体と符号　：　有限体
【第7回】　有限体と符号　：　ハミング符号
【第8回】　有限体と符号　：　巡回符号
【第9回】　有限体と符号　：　BCH符号
【第10回】　整数論と暗号　：　暗号、整数、素数と素因数分解
【第11回】　整数論と暗号　：　ユークリッドの互除法
【第12回】　整数論と暗号　：　1次不定方程式
【第13回】　整数論と暗号　：　合同式
【第14回】　整数論と暗号　：　フェルマーの小定理
【第15回】　整数論と暗号　：　RSA暗号