

|                                                                                                            |                                                                                                                           |                          |                   |                          |                                                        |                           |     |
|------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|--------------------------|-------------------|--------------------------|--------------------------------------------------------|---------------------------|-----|
| 徳山工業高等専門学校                                                                                                 |                                                                                                                           | 開講年度                     | 平成29年度 (2017年度)   |                          | 授業科目                                                   | 離散数学                      |     |
| 科目基礎情報                                                                                                     |                                                                                                                           |                          |                   |                          |                                                        |                           |     |
| 科目番号                                                                                                       | 0025                                                                                                                      |                          |                   | 科目区分                     | 専門 / 選択                                                |                           |     |
| 授業形態                                                                                                       | 講義                                                                                                                        |                          |                   | 単位の種別と単位数                | 学修単位: 2                                                |                           |     |
| 開設学科                                                                                                       | 機械制御工学専攻                                                                                                                  |                          |                   | 対象学年                     | 専2                                                     |                           |     |
| 開設期                                                                                                        | 前期                                                                                                                        |                          |                   | 週時間数                     | 2                                                      |                           |     |
| 教科書/教材                                                                                                     | 講義ノート：必要に応じて資料を配布する。                                                                                                      |                          |                   |                          |                                                        |                           |     |
| 担当教員                                                                                                       | 義永 常宏                                                                                                                     |                          |                   |                          |                                                        |                           |     |
| 到達目標                                                                                                       |                                                                                                                           |                          |                   |                          |                                                        |                           |     |
| 整数論の基礎とそれが暗号理論にどのように用いられているのか、また、誤り訂正符号の考え方、特に、ガロア体とその拡大体がBCH符号にどのように応用されているのか、に関する基本・基礎的事項の理解・修得が到達目標である。 |                                                                                                                           |                          |                   |                          |                                                        |                           |     |
| ルーブリック                                                                                                     |                                                                                                                           |                          |                   |                          |                                                        |                           |     |
|                                                                                                            |                                                                                                                           | 理想的な到達レベルの目安             |                   | 標準的な到達レベルの目安             |                                                        | 未到達レベルの目安                 |     |
|                                                                                                            |                                                                                                                           | 整数の諸性質の証明と平文の暗号化・復号ができる。 |                   | 平文の暗号化および復号ができる          |                                                        | 平文の暗号化および復号ができない。         |     |
|                                                                                                            |                                                                                                                           | ガロア体、情報の符号化、誤り訂正を応用できる。  |                   | ガロア体の計算、情報の符号化、誤り訂正ができる。 |                                                        | ガロア体の計算、情報の符号化、誤り訂正ができない。 |     |
| 学科の到達目標項目との関係                                                                                              |                                                                                                                           |                          |                   |                          |                                                        |                           |     |
| JABEE c-1<br>到達目標 A 1                                                                                      |                                                                                                                           |                          |                   |                          |                                                        |                           |     |
| 教育方法等                                                                                                      |                                                                                                                           |                          |                   |                          |                                                        |                           |     |
| 概要                                                                                                         | 実際の情報技術と関連付けながら、整数の基本理論と暗号理論への応用、ガロア体の理論の基本事項と符号理論への応用について学習する。これまでに学んできた数学とは違ったタイプとなるため、難しいと感じるかもしれないが、こうした思考力も是非養って欲しい。 |                          |                   |                          |                                                        |                           |     |
| 授業の進め方・方法                                                                                                  | 講義が主体であるが、輪講形式や学習シートとして事前に割り当てた演習問題の解答を板書してもらうことも取り入れる。授業内容を理解するためには自学が必要である。                                             |                          |                   |                          |                                                        |                           |     |
| 注意点                                                                                                        | 【関連科目】 本科：集合と論理（2年）、数学IIIB（3年）、情報数学（3年）                                                                                   |                          |                   |                          |                                                        |                           |     |
| 授業計画                                                                                                       |                                                                                                                           |                          |                   |                          |                                                        |                           |     |
|                                                                                                            |                                                                                                                           | 週                        | 授業内容              |                          | 週ごとの到達目標                                               |                           |     |
| 前期                                                                                                         | 1stQ                                                                                                                      | 1週                       | オリエンテーションと整数(1)   |                          | オリエンテーションの後、整数の初歩・基本的な諸概念および必要な記法について学ぶ。               |                           |     |
|                                                                                                            |                                                                                                                           | 2週                       | 整数（2）             |                          | 素因数分解が一意的であること、および素数が無限に存在すること、合同式について学ぶ。              |                           |     |
|                                                                                                            |                                                                                                                           | 3週                       | 整数（3）             |                          | 合同式と解、最小正剰余、及びフェルマーの(小)定理、Nを法とする行列について学ぶ。              |                           |     |
|                                                                                                            |                                                                                                                           | 4週                       | Nを法とする一次変換と暗号への応用 |                          | まず、暗号の概略を説明した後に、Nを法とする正則行列とその暗号への応用について学ぶ。             |                           |     |
|                                                                                                            |                                                                                                                           | 5週                       | RSA暗号（1）          |                          | 公開鍵暗号の考え方と現在最も有名な暗号の1つであるRSA暗号の構成方法について学ぶ。             |                           |     |
|                                                                                                            |                                                                                                                           | 6週                       | RSA暗号（2）          |                          | 平文の暗号・復号の例を通じて、RSA暗号についての理解を深める。                       |                           |     |
|                                                                                                            |                                                                                                                           | 7週                       | 符号                |                          | 符号の原理、誤り検出・訂正のアイデアとその限界、及びハミング距離等について学習する。             |                           |     |
|                                                                                                            |                                                                                                                           | 8週                       | ガロア体（1）           |                          | ガロア体の定義や演算、及びガロア体上の規約多項式について理解する。                      |                           |     |
|                                                                                                            | 2ndQ                                                                                                                      | 9週                       | ガロア体（2）           |                          | ガロア体の2次拡大体の定義、構成法、線形表現と累乗表現について学ぶ。                     |                           |     |
|                                                                                                            |                                                                                                                           | 10週                      | ガロア体（3）           |                          | ガロア体の3次および4次拡大体について学ぶ。                                 |                           |     |
|                                                                                                            |                                                                                                                           | 11週                      | パリティ検査符号とハミング符号   |                          | パリティ検査符号の考え方と拡張としてのハミング符号についての誤り訂正の原理について学ぶ。           |                           |     |
|                                                                                                            |                                                                                                                           | 12週                      | 巡回符号              |                          | 符号多項式、および、巡回符号の定義、性質、生成多項式、シンドロームについて学習する。             |                           |     |
|                                                                                                            |                                                                                                                           | 13週                      | BCH符号（1）          |                          | ガロア体と拡大体を巧みに用いたBCH符号の定義とその生成多項式について学ぶ。なお例では、4次拡大体を用いる。 |                           |     |
|                                                                                                            |                                                                                                                           | 14週                      | BCH符号（2）          |                          | BCH符号における誤り訂正について学ぶ。                                   |                           |     |
|                                                                                                            |                                                                                                                           | 15週                      | 期末試験              |                          | 整数の基礎理論と暗号理論、ガロア体と符号理論についての理解をチェックする。                  |                           |     |
|                                                                                                            |                                                                                                                           | 16週                      | まとめ               |                          | 試験の解説と授業のまとめを行う。                                       |                           |     |
| モデルコアカリキュラムの学習内容と到達目標                                                                                      |                                                                                                                           |                          |                   |                          |                                                        |                           |     |
| 分類                                                                                                         | 分野                                                                                                                        | 学習内容                     | 学習内容の到達目標         |                          |                                                        | 到達レベル                     | 授業週 |
| 評価割合                                                                                                       |                                                                                                                           |                          |                   |                          |                                                        |                           |     |
|                                                                                                            | 試験                                                                                                                        | 発表                       | 相互評価              | 態度                       | ポートフォリオ                                                | その他                       | 合計  |
| 総合評価割合                                                                                                     | 100                                                                                                                       | 0                        | 0                 | 0                        | 0                                                      | 0                         | 100 |
| 基礎的能力                                                                                                      | 0                                                                                                                         | 0                        | 0                 | 0                        | 0                                                      | 0                         | 0   |
| 専門的能力                                                                                                      | 100                                                                                                                       | 0                        | 0                 | 0                        | 0                                                      | 0                         | 100 |
| 分野横断的能力                                                                                                    | 0                                                                                                                         | 0                        | 0                 | 0                        | 0                                                      | 0                         | 0   |