離散数学 (Discrete Mathematics)

専攻	選択・必修	開設時期	単位数	授業形態	担　当
専門基礎	選択	2 年前	2	講義	義永常宏

【授業の概要】
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、及び、ガロア体の理論の基本事項と符号理論について学習する。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、あるいは、戸惑いを覚えるかもしれないが、こうした思考力も是非養って欲しい。

【学修の進め方】
座学の他、適宜、輪講形式も取り入れ、割り当てた範囲を担当してもらう。また、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ある。従って、自学による予習・復習が必要とされる。

【授業の概要】	【授業項目】	【内　容】
1 回	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。（学習シート）
2 回	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 回	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 を法とする行列ついて学ぶ。
4 回	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述べる。（学習シート）
5 回	RSA 暗号（１）	公開鍵暗号の考え方と現在最もよく用いられているＲＳＡ暗号の構成方法について学ぶ。
6 回	RSA 暗号（２）	例を通じて、RSA 暗号についての理解を深める。
7 回	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。（学習シート）
8 回	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説明する。
9 回	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 回	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 回	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 回	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。（学習シート）
13 回	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。例では、4 次拡大体を用いる。
14 回	BCH 符号（２）	ＢＣＨ符号における誤り訂正について学ぶ。
15 回	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 回	まとめ	試験の解説と授業のまとめを行う。

【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。

【徳山高専学習・教育目標】	Ａ１	【ＪＡＢＥＥ基準 1(1)】	c-1

【評価法】	期末試験で評価する。
【テキスト】	参考図書：情報数学の基礎（寺田文行他著）サイエンス社 情報・符号・暗号の理論入門（守屋悦朗）サイエンス社
【関連科目】	本科：集合と論理（2 年）、数学 IIIB（3 年）、情報数学（3 年）

【成績欄】	前期中間試験【　　】　前期末試験【　　】　前期成績【　　】　後期中間試験【　　】　後期末試験【　　】　学年末成績【　　】