高知工業高等専門学校	開講年度	令和06年度 (2024年度)	授業科目	情報代数

科目基礎情報

科目番号	I3035	科目区分	専門 / 必修
授業形態	講義	単位の種別と単位数	履修単位: 1
開設学科	SD 情報セキュリティコース	対象学年	3
開設期	前期	週時間数	2
教科書/教材	教材はオリジナルのものを作成し配布する		
担当教員	立川 崇之		

到達目標

1. 集合・命題・論理式等の基本概念を理解し，具体的な問題を解くことができる.
2. 群・環・体の概念とその基礎的な性質を理解する.
3. 有限体の理論の初歩を学び，暗号あるいは符号理論への応用についてもその原理を理解することができる.
4. 論理演算を行うことができる.

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
評価項目1	確率的整数論により巨大な整数を素数判定する方法を理解し，素数判定するプログラムを構築できる。	確率的整数論により巨大な整数を素数判定する方法を説明できる。	確率的整数論により巨大な整数を素数判定する方法が説明できない。
評価項目2	群・環・体の概念とその基礎的な性質を理解し，集合演算および集合の間の関数演算ができる。	群・環・体の概念とその基礎的な性質を理解し，集合演算ができる。	群・環・体の概念とその基礎的な性質を理解できず，集合演算ができない。
評価項目３	論理演算，論理式の表現を行うことができ、冗長な論理式を簡単化することができる。	論理演算，論理式の表現を行うことができる。	論理演算，論理式の表現を行うことができない。

学科の到達目標項目との関係

学習・教育到達度目標 (C)

教育方法等

概要	暗号理論，符号理論の基礎となる確率的整数論，群・環・体の基本的な性質を，具体例を踏まえて理解することを目指す．また，論理回路で行われる演算である論理演算（AND, OR, NOT）について理解する．これにより，今後学習する暗号理論，符号理論，論理回路の基本的知識を習得することを目指す。これらの学習と並行して，プログラムへの暗号化処理の実装方法について，基本的知識を習得する.
授業の進め方・方法	教材は市販の教科書を使用せず，独自に作成したものを印刷し配布する．授業では教材に沿ってポイントを説明する．学生はノートを取り，わからないことがあれば，時間中あるいは授業時間外に質問する．講義のポイントとなるところでレポート課題を出題し，その提出状況を評価に反映する．定期試験も実施する. 進行状況や理解度により「群の準同型、同型」「コーシーの定理」の取り扱いは教材配布のみとし，既習の数学や物理学，情報工学などと関わる群の具体的な例を多く取り上げることがある.
注意点	【成績評価の基準・方法】 試験の成績を90%，課題を10%の割合で総合的に評価する．成績評価は中間と期末の各期間の評価の平均とする．学年の評価は後学期末の評価とする．技術者が身に着けるべき専門基礎として，上記の到達目標に対する達成度を試験等において評価する. 【事前・事後学習】 事前学習として配布した教材を読んだ上で，理解が難しかった部分を整理して授業に臨むこと．また，事後学習として授業内で取り扱った項目について練習問題を複数回解き理解を深めること. 【履修上の注意】 本科目では2年生までの数学と異なり，抽象的な考え方がたびたび現れる．具体例を交えて説明するが，分からないところがあれば積極的に質問をしてもらいたい．また，教材についても分かりにくいところなどがあれば指摘してもらいたい．レポート課題はコンピュータを用いて解くものが含まれ，2年生までで既習のプログラミング言語では解答が困難なものがあると想定されるため，Python など新たな言語の利用にも積極的に取り組む姿勢を持ってもらいたい.

授業の属性・履修上の区分

☐ アクティブラーニング	☐ ICT 利用	☐ 遠隔授業対応	☐ 実務経験のある教員による授業

授業計画

		週	授業内容	週ごとの到達目標
前期	1stQ	1週	ガイダンス ユークリッドの互除法	授業の進め方，評価法などについて理解する. 2年生で既習のユークリッドの互助法について復習する.
		2週	合同式	整数の除算における余りの関係に着目する，合同式の性質について理解する.
		3週	フェルマーの小定理	素数に関する合同式の定理である，フェルマーの小定理の証明と意味を理解する.
		4週	フェルマーテスト	フェルマーの小定理の対偶を取った命題から考えられた，素数判定の確率的手法であるフェルマーテストを理解する.
		5週	ミラー・ラビンテスト	フェルマーテストで見落としてしまう擬素数を合成数と判定できる，ミラー・ラビンテストについて理解する.
		6週	整数，有理数，実数，複素数の演算	群，環，体の導入として，整数，有理数，実数，複素数とその演算の性質を復習する.
		7週	論理演算入門	0と1だけからなる集合に対し，論理積 (AND)，論理和 (OR)，否定 (NOT) などの演算を理解する.
		8週	論理式の変換、ド・モルガンの法則	論理式の変換法則、ド・モルガンの法則を扱い、複雑な論理式を同値の簡単化された式に変形する方法を理解する。
	2ndQ	9週	群，環，体の基本性質	集合と演算の規則から定義される群，環，体について，実数などの具体的な集合を踏まえて理解する.

		10週	剰余環、巡回群	有限個の元からなる剰余環、巡回群について、基本的な性質と演算の規則について理解する。
		11週	剰余環の除法、乗法群	剰余環の除法を用いた合同方程式の解法、剰余環の乗法群について理解する。
		12週	置換群、部分群	二つの集合間で、順序を入れ替える写像である、置換について理解する。 群の空で無い部分集合である部分群について、基本的な性質を学習する。
		13週	群の準同型、同型，コーシーの定理	２つの群の写像について、特別な性質をもつ準同型、同型について具体例を踏まえて理解する。位数nの有限群に対し、nの素因数pを位数に持つ有限群が存在するという、コーシーの定理について学習する。
		14週	いろいろな群1	既習の数学などについて、直交群や非可換群の観点から解説する。
		15週	いろいろな群2	既習の数学などについて、直交群や非可換群の観点から解説する。
		16週		

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
基礎的能力	数学	数学	数学	整式の加減乗除の計算や、式の展開ができる。	3	
				因数定理等を利用して、4次までの簡単な整式の因数分解ができる。	3	
				分数式の加減乗除の計算ができる。	3	
				実数・絶対値の意味を理解し、絶対値の簡単な計算ができる。	3	
				平方根の基本的な計算ができる(分母の有理化も含む)。	3	
				複素数の相等を理解し、その加減乗除の計算ができる。	3	
				解の公式等を利用して、2次方程式を解くことができる。	3	
				因数定理等を利用して、基本的な高次方程式を解くことができる。	3	
				簡単な連立方程式を解くことができる。	3	
				無理方程式・分数方程式を解くことができる。	3	
				1次不等式や2次不等式を解くことができる。	3	
				恒等式と方程式の違いを区別できる。	2	
				2次関数の性質を理解し、グラフをかくことができ、最大値・最小値を求めることができる。	3	
				分数関数や無理関数の性質を理解し、グラフをかくことができる。	3	
				簡単な場合について、関数の逆関数を求め、そのグラフをかくことができる。	3	
				累乗根の意味を理解し、指数法則を拡張し、計算に利用することができる。	3	
				指数関数の性質を理解し、グラフをかくことができる。	3	
				指数関数を含む簡単な方程式を解くことができる。	3	
				対数の意味を理解し、対数を利用した計算ができる。	3	
				対数関数の性質を理解し、グラフをかくことができる。	3	
				対数関数を含む簡単な方程式を解くことができる。	3	
				角を弧度法で表現することができる。	3	
				三角関数の性質を理解し、グラフをかくことができる。	3	
				加法定理および加法定理から導出される公式等を使うことができる。	3	
				三角関数を含む簡単な方程式を解くことができる。	3	
				2点間の距離を求めることができる。	3	
				内分点の座標を求めることができる。	3	
				2つの直線の平行・垂直条件を利用して、直線の方程式を求めることができる。	2	
				簡単な場合について、円の方程式を求めることができる。	3	
				積の法則と和の法則を利用して、簡単な事象の場合の数を数えることができる。	2	
				簡単な場合について、順列と組合せの計算ができる。	3	
				等差数列・等比数列の一般項やその和を求めることができる。	3	
				総和記号を用いた簡単な数列の和を求めることができる。	3	
				不定形を含むいろいろな数列の極限を求めることができる。	3	
				無限等比級数等の簡単な級数の収束・発散を調べ、その和を求めることができる。	3	
				ベクトルの定義を理解し、ベクトルの基本的な計算(和・差・定数倍)ができ、大きさを求めることができる。	3	
				平面および空間ベクトルの成分表示ができ、成分表示を利用して簡単な計算ができる。	3	
				平面および空間ベクトルの内積を求めることができる。	3	
				問題を解くために、ベクトルの平行・垂直条件を利用することができる。	3	

				空間内の直線・平面・球の方程式を求めることができる(必要に応じてベクトル方程式も扱う)。	3	
				行列の定義を理解し、行列の和・差・スカラーとの積、行列の積を求めることができる。	2	
				逆行列の定義を理解し、2次の正方行列の逆行列を求めることができる。	3	
				行列式の定義および性質を理解し、基本的な行列式の値を求めることができる。	3	
				線形変換の定義を理解し、線形変換を表す行列を求めることができる。	2	
				合成変換や逆変換を表す行列を求めることができる。	3	
				平面内の回転に対応する線形変換を表す行列を求めることができる。	3	
				簡単な場合について、関数の極限を求めることができる。	3	
				微分係数の意味や、導関数の定義を理解し、導関数を求めることができる。	3	
				積・商の導関数の公式を用いて、導関数を求めることがができる。	3	
				合成関数の導関数を求めることができる。	3	
				三角関数・指数関数・対数関数の導関数を求めることができる。	3	
				逆三角関数を理解し、逆三角関数の導関数を求めることができる。	3	
				関数の増減表を書いて、極値を求め、グラフの概形をかくことができる。	3	
				極値を利用して、関数の最大値・最小値を求めることができる。	3	
				簡単な場合について、関数の接線の方程式を求めることができる。	2	
				2次の導関数を利用して、グラフの凹凸を調べることができる。	3	
				関数の媒介変数表示を理解し、媒介変数を利用して、その導関数を求めることができる。	3	
				不定積分の定義を理解し、簡単な不定積分を求めることができる。	2	
				置換積分および部分積分を用いて、不定積分や定積分を求めることができる。	3	
				定積分の定義と微積分の基本定理を理解し、簡単な定積分を求めることができる。	2	
				分数関数・無理関数・三角関数・指数関数・対数関数の不定積分・定積分を求めることができる。	3	
				簡単な場合について、曲線で囲まれた図形の面積を定積分で求めることができる。	3	
				簡単な場合について、曲線の長さを定積分で求めることができる。	3	
				簡単な場合について、立体の体積を定積分で求めることができる。	3	
				2変数関数の定義域を理解し、不等式やグラフで表すことができる。	2	
				合成関数の偏微分法を利用して、偏導関数を求めることができる。	3	
				簡単な関数について、2次までの偏導関数を求めることができる。	3	
				偏導関数を用いて、基本的な2変数関数の極値を求めることができる。	3	
				2重積分の定義を理解し、簡単な2重積分を累次積分に直して求めることができる。	2	
				極座標に変換することによって2重積分を求めることができる。	3	
				2重積分を用いて、簡単な立体の体積を求めることができる。	3	
				微分方程式の意味を理解し、簡単な変数分離形の微分方程式を解くことができる。	2	
				簡単な1階線形微分方程式を解くことができる。	3	
専門的能力	分野別の専門工学	情報系分野	情報数学・情報理論	集合に関する基本的な概念を理解し、集合演算を実行できる。	4	前9,前10
				集合の間の関係(関数)に関する基本的な概念を説明できる。	4	前9,前12,前13
				ブール代数に関する基本的な概念を説明できる。	3	前7,前8
				論理代数と述語論理に関する基本的な概念を説明できる。	3	前7,前8
				情報源のモデルと情報源符号化について説明できる。	2	前1
				通信路のモデルと通信路符号化について説明できる。	2	前1

評価割合

	試験	発表	相互評価	態度	ポートフォリオ	課題	合計
総合評価割合	90	0	0	0	0	10	100
基礎的能力	50	0	0	0	0	5	55
専門的能力	30	0	0	0	0	5	35
分野横断的能力	10	0	0	0	0	0	10