

鹿児島工業高等専門学校		開講年度	平成30年度 (2018年度)		授業科目	応用代数学	
科目基礎情報							
科目番号	0037		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	電気情報システム工学専攻		対象学年		専2		
開設期	後期		週時間数		2		
教科書/教材	〔教科書〕 なし／〔参考書・補助教材〕 図書館の参考書類（整数論，暗号で検索），配布するプリント類						
担当教員	白坂 繁						
到達目標							
(1) 代数的な考え方・論理的な思考を修得すること。 (2) 具体的な計算処理に習熟すること。 (3) 抽象的な概念を理解し，応用できること。							
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. 互除法を使用して、最大公約数を求めることができる。		互除法により、最大公約数を求め、更に一次不定方程式の一般解を求めることができる。		最大公約数・最小公倍数を理解し、互除法により、最大公約数を求めることができる。		互除法により、最大公約数を求めることができない。	
評価項目2. オイラー関数の値を求め、合同式が解ける。		合同式とオイラーの関数の値より、オイラーの定理の計算ができる。		合同式が解け、オイラーの関数の値を求めることができる。		合同式が解け、オイラーの関数の値を求めることができない。	
評価項目3. R S A暗号の基本的仕組みを理解できる。		R S A暗号の仕組みを理解し、暗号化・復号化の計算ができ、解読が困難なことを説明できる。		合同式を利用して、R S A暗号の仕組みを理解し、暗号化・復号化の計算ができる。		R S A暗号の暗号化・復号化の計算ができない。	
評価項目4. 群論の初歩と抽象的数学の考え方を理解できる。		群論を理解し、実際の問題に応用・適用できる。抽象的な記述・証明を理解できる。		群論の計算と、構造を理解し、簡単な群の説明ができる。		群の計算ができない。	
学科の到達目標項目との関係							
教育方法等							
概要		(1) 本科までの論理的な考え方を前提とする。 (2) 本科目は，専門科目や将来の職業のための基礎科目として位置付けられる。					
授業の進め方・方法		講義・演習方式で行う					
注意点		(1) 集中すべきときに集中して要点をつかみ，理解すべきことを確実に理解すること。 (2) 講義内容をよりよく理解するために，毎回，教科書等を参考に2時間程度の予習をしておくこと。 (3) 課題等の演習問題で，2時間以上の反復練習をし，抽象的な思考に慣れること。 (4) 疑問点は，その都度，質問すること。					
授業計画							
		週	授業内容		週ごとの到達目標		
後期	3rdQ	1週	1. 初等整数論		☐ ①最大公約数と最小公倍数との関係を理解できる。		
		2週	1. 初等整数論		☐ ②互除法により最大公約数 を求めることができる。		
		3週	1. 初等整数論		☐ ③互除法により，一次不定方程式 が解ける。		
		4週	2. 合同式		☐ ①合同式とその性質 を理解 できる。		
		5週	2. 合同式		☐ ②連立一次合同式 が解ける。		
		6週	2. 合同式		☐ ③オイラーの関数の値 を求めることができる。		
		7週	2. 合同式		☐ ③オイラーの関数の値 を求めることができる。		
		8週	2. 合同式		☐ ④オイラーの (小) 定理 の計算ができる。		
	4thQ	9週	3. R S A暗号		☐ ①公開鍵暗号の仕組み を理解できる。		
		10週	3. R S A暗号		☐ ②暗号化・復号化のアルゴリズム を理解できる。		
		11週	4. 群論		☐ ①群の定義とその例 を理解できる。 ☐ ②部分群の性質 を定義に基づいて理解できる。		
		12週	4. 群論		☐ ③正規部分群の性質 を定義に基づいて理解できる。		
		13週	4. 群論		☐ ④群の準同形定理 を理解できる。		
		14週	4. 群論		☐ ⑤群論を実際の問題 に応用できる。		
		15週	試験答案返却・解説		試験において、間違えた部分を自分の課題として把握する（非評価項目）。		
		16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	75	0	0	0	0	25	100
基礎的能力	75	0	0	0	0	25	100
専門的能力	0	0	0	0	0	0	0
分野横断的能力	0	0	0	0	0	0	0