

科目名	応用数学Ⅱ			担当教員	奥山真吾		
学年	電子制御工学科5年	学期	通年	履修条件	必修	単位数	2
分野	専門	授業形式	講義	科目番号	07C05_30020		
学習目標	群や体という代数学の基本的概念を習得し、暗号理論への応用について理解することを目標とする。特に、群論においては位数の低いものや、対称群、多面体群などについて、乗積表やそれらの間の準同型について学び、具体的に理解することを目指す。また、剰余の計算や多項式環における計算を通じて環や体の概念の習得を目指す。さらに、楕円曲線について学び、暗号理論の基礎と発展について理解することを目標とする。						
進め方	プリントを配布し、それに沿って進める。定期的に課題演習を行い、理解を深める。具体的な例について計算することに重点を置き、直観的に内容を理解できるように配慮する。また、定期的にレポート課題を課す。						
履修要件	特になし						
学習内容	学習項目（時間数）			学習到達目標			
	1. 集合・論理(2)			集合と論理の記号の意味がわかる	D1:1		
	2. 群の定義(2)			群であるかどうか判定できる	D1:2		
	3. 群の同型と乗積表(2)			乗積表の意味がわかる	D1:2		
	4. 課題演習(2)						
	5. 位数の小さな群(2)			位数の小さな群の乗積表が書ける	D1:2		
	6. 対称群・交代群(2)			対称群・交代群の計算ができる	D1:2		
	7. 正多面体群(2)			正多面体群の乗積表がかけられる	D1:2		
	8. 前期中間試験(2)						
	9. 線形群(2)			行列の集合の群構造が分かる	D1:2		
	10. 準同型写像(2)			準同型写像であるかどうか判定できる	D1:2		
	11. 部分群(2)			部分群が求められる	D1:3		
	12. 課題演習(2)						
	13. 準同型定理(2)			準同型定理が理解できる	D1:3		
	14. 群の間の関係(2)			複数の群の間の関係が理解できる	D1:3		
	15. 前期期末試験(2)						
	16. 試験問題の解答と授業評価アンケート(2)			剰余の計算ができる	D1:3		
	17. 剰余の計算			加群であるかどうか判定できる	D1:2		
	18. 加群			アーベル群の基本定理理解している	D1:2		
	19. アーベル群の基本定理						
	20. 課題演習			環・体であるかどうか判定できる	D1:2		
	21. 環・体の定義			ユークリッドの互除法が適用できる	D1:3		
	22. ユークリッドの互除法						
	23. 後期中間試験(2)						
	24. ベクトル空間(4)			ベクトル空間について知っている	D1:1		
	25. 多項式環(4)			多項式環の構造を知っている	D1:2		
	26. 代数拡大(4)			代数拡大の基本的事項を知っている	D1:2		
	27. 課題演習						
	28. 楕円曲線(4)			楕円曲線の与える群構造が説明できる	D1:2		
	29. 暗号理論(4)			暗号の仕組みが説明できる	D1:2		
	30. 学年末試験(2)						
31. 試験問題の解答と授業評価アンケート(2)							
評価方法	中間試験・期末試験70%、レポート・演習30%の比率で総合評価する。						
関連科目							
教材	プリント配布						
備考	特になし						