

## 課程大綱及進度表

開課系所	應用數學所
開課學年	99
開課學期	1
課程名稱(中文)	有限體
課程名稱 (英文)	FINITE FIELDS
課程碼	L154600
分班碼	
先修科目或先備能力	代數(一)(二)
學分數	3
開課教師	柯文峰
e-mail	<a href="mailto:wfke@mail.ncku.edu.tw">wfke@mail.ncku.edu.tw</a>
電話	65154
Office Hours	
課程概述 (中文、英文)	由於有限體有著廣泛的應用，如組合學、編碼學、密碼學、及電路學等，它是相當熱門的一個學問。我們將介紹這個理論的基礎，並將重點放在應用的實用性上頭。數學上的應用如有限幾何、組合學、及類亂數產生器等，也會課程中接觸到。最後介紹其在資訊學上的應用，尤其是代數編碼及密碼上的應用。
教學目標	<ol style="list-style-type: none"> <li>1. 有限體的代數結構及性質。</li> <li>2. 有限體在資訊學上的應用。</li> <li>3. 有限體在數學上的應用。</li> </ol>
授課課程大綱明細	<ol style="list-style-type: none"> <li>1. Algebraic foundations</li> <li>2. Structure of finite fields</li> <li>3. Polynomials over finite fields</li> <li>4. Factorization of polynomials</li> <li>5. Exponential sums</li> </ol>

	6. Linear recurring sequences 7. Theoretical applications of finite fields 8. Algebraic coding theory 9. Cryptology
參考書目	Introduction to Finite Fields and their Applications, 2 <sup>nd</sup> Edition (Rudolf Lidl and Harald Niederreiter)
課程要求	1. 課堂上課 2. 期中及期末考試 3. 作業
評量方式	1. 期中考試 (40%) 2. 期末考試 (40%) 3. 作業及平時上課狀況 (20%)
課程網址	
助教資訊	無
備註	