東海大學數學研究所

碩士論文

布 p 環的研究

On the Boolean p-Ring

研 究 生 ： 董 又 誠（Yu-Chen Tung）

指 導 教 授 ： 沈 淵 源（Yuan-Yuan Shen）

中 華 民 國 九 十 九 年 六 月

布 p 環的研究

On the Boolean p-Ring

研 究 生 ： 董又誠 Student ： Yu-Chen Tung

指 導 教 授 ： 沈淵源 Advisor ： Yuan-Yuan Shen

東海大學

數學系

碩士論文

A Thesis

Submitted to Institute of Applied Mathematics

College of Science

Tunghai University

in Partial Fulfillment of the Requirements

for the Degree of

Master of Science

In Mathematics

June 2010

Taichung Taiwan, Republic of China.

中華民國九十九年六月

東 海 大 學

數 學 系

碩士學位口試委員審定書

本系碩士班 董又誠 君

所提論文 On the Boolean p-rings
（布 p 環的研究）

合於碩士班資格水準，業經本委員會評審通過，特此證明

口試委員：

指導教授：

所 長：

中 華 民 國 九十九 年 六 月 十九 日

誌　　謝

本篇文章能夠完成, 要特別感謝我最敬愛的指導老師沈淵源教授, 對我的照顧與指導。在沈淵源老師耐心的指導下, 讓我瞭解數學與環可以這麼有趣來發揚其精神與內涵。

我無法戮力以赴, 因帶重責重職 ， 學校、家庭、數研所三頭燒，心有餘而力不足。為求助益往後社會、人類之人生, 開創新紀元或更遠程的明天而努力, 探索志趣之深潛 , 也得於時間、於體力化零為整, 以明志、略達心願。

總之, 要感謝家人的支持、數研院所的恩師們極力激勵與栽培, 銘感心內。惟日後更努力、更上進來答報深謝。

董 又 誠　　謹 識 於

東 海 大 學 數 學 系

中華民國九十九年六月

目　　錄

摘　　要

令 $p \geq 2$ 爲一整數。我們稱一個環爲布 p 環,若滿足

$$x^p = x, \ \forall x \in R \text{。}$$

到底哪些布 p 環是交換環呢？在本論文中，我們將做一初步的探討。

第一章 代數結構簡介

一個集合若沒有二元運算,那就沒什麼代數結構可言。不具任何研究的價值。令$*$爲集合S上的一個二元運算。

・我們說運算$*$是可結合的（associative）；若

$$(a*b)*c=a*(b*c),\forall a,b,c\in S \text{ 。}$$

・我們說運算$*$是可交換的（commutative）；若

$$a*b=b*a,\forall a,b,c\in S \text{ 。}$$

・集合S中的一個元素e 稱之爲運算$*$的一個單位元素（identity element）；若

$$a*e=e*a=a,\forall a\in S \text{ 。}$$

・集合S擁有運算$*$的一個單位元素e；則我們說元素$u\in S$在集合S中具有反元素（inverse），如果存在$v\in S$ 使得

$$u*v=v*u=e \text{ 。}$$

在複數集C中有兩個我們熟悉的二元運算加（＋）與乘（・）；就是這兩個二元運算使得複數集C擁有豐富的代數結構。

（i）加法運算（＋）在C上具有封閉性、結合性、單位元素$0+0i$,而且每一個元素$a+bi$都有反元素$(-a)+(-b)i$,這就是所謂的群（group）的結構。

一般而言,集合S上的二元運算$*$；若滿足上述四個性質,我們就說S在運算$*$之下形成一個群或說$(S,*)$是一個群。如果運算$*$是可交換的；那麼理所當然 ,我們就說 $(S,*)$是一個交換群（commutative group）。通常又稱爲阿貝爾群（abelian group）,爲的是要紀念數學家阿貝爾。$(C,+)$當然是一個阿貝爾群。

（ii）乘法運算（ • ）在C上具有封閉性、結合性、單位元素$1+0i$,而且每一個非零元素$a+bi\neq 0$都有反元素$\frac{a}{a^2+b^2}+\frac{-b}{a^2+b^2}i$,又乘法亦可交換；也就是說,$(C\setminus\{0\},\cdot)$是一個阿貝爾群。

（iii）這兩個運算,並不是獨立存在毫無關連的；其相關性就是所謂的對＋的分配律,即

$$\alpha\cdot(\beta+\gamma)=\alpha\cdot\beta+\alpha\cdot\gamma,\forall\alpha,\beta,\gamma\in C$$

這就是所謂體（field）的代數結構。一般而言,擁有兩個運算$*_1,*_2$的集合S；若滿足上述C之性質者,我們就說S在運算$*_1,*_2$之下形成一個體或說（$S,*_1,*_2$）是一個體。更明確的說,令$*_1,*_2$爲集合S的二元運算；我們會說（$S,*_1,*_2$）是一個體,若滿足下述三個性質：

（i）（$S,*_1$）是一個阿貝爾群。

（ii）（$S\setminus\{e_1\},*_2$）也是阿貝爾群,此處e_1爲$*_1$的單位元素。

（iii）運算$*_2$對運算$*_1$的分配律成立：

$$a*_2(b*_1c)=(a*_2b)*_1(a*_2c),\forall a,b,c\in S$$

我們所熟悉的例子當中,除了有理數體、實數體以及複數體之外；

$$(\ Q\ ,\ +\ ,\ \cdot\ )\ \subset\ (\ R\ ,\ +\ ,\ \cdot\ )\ \subset\ (\ C\ ,\ +\ ,\ \cdot\ )$$

還有那些介於有理數體及複數體之間的數體（number field）,更有那數也數不清的質數個數的有限體（finite fields）Z_p。

前面的整數系$(\ Z\ ,\ +\ ,\ \cdot\ )$遠比一般的環還好很多；那就是第二個運算不僅有單位元素,而且還是可交換的,此種環通常稱之爲具單位元素的交換環（commutative ring with unit）。與此相對的有n階方陣環$(M_n(R),\ +\ ,\ \cdot\ )$,此爲具單位元素的非交換環（ noncommutative ring with unit ）。

其實,整數環還有好的性質；譬如說,任何兩個非零元素相乘還是非零元素,這就是所謂的整域（integral domain）的代數結構。但是,一般的環,如Z_6就包含有非零元素 2 及 3 相乘之後等於零；還有矩陣環中,

$$\begin{pmatrix} 3 & 7 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 7 \\ 0 & -3 \end{pmatrix}=\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

也有類似的現象發生。

第二章 環的基本性質與例子

第一節 基本定義與性質

（一）環的定義：非空集環R在加（＋）、乘（・）運算之下,滿足：

1. $(R,+)$是一個交換群。
2. $(ab)c=a(bc),\forall a,b,c\in R$（乘法結合律）
3. $a(b+c)=ab+ac$ 及 $(a+b)c=ac+bc$（左及右分配律）

若以上三個條件,再加入下面第 4 個條件：

4. $ab=ba,\forall a,b\in R$,

就稱爲交換環。

（二）基本性質

若R是一個環,則我們有

1. $0a=a0=0,\forall a\in R$ ；
2. $(-a)b=a(-b)=-(ab),\forall a,b\in R$；
3. $(-a)(-b)=ab,\forall a,b\in R$；
4. $(na)b=a(nb)=n(ab),\forall n\in Z$ 及$\forall a,b\in R$ ；
5. $(\sum_{i=1}^{n}a_i)(\sum_{j=1}^{m}b_j)=\sum_{i=1}^{n}\sum_{j=1}^{m}a_ib_j,\forall a_i,b_j\in R$。

第二節 例子

例 1：整數 Z 在一般的加法與乘法之下形成一個交換環。

例 2：佈於實數（或複數）的多項式 $R[x]$(或 $C[x]$)在一般的加法與乘法之下形成一個交換環。

例 3：令 $M_n(R)$ 爲佈於實數體的 n 階方陣,則 $M_n(R)$ 在一般的加法與乘法之下形成一個環,但不是交換環。

例 4：令 S 爲一個集合,且 $\wp(S)$ 爲所有 S 的子集合所形成的集合。我們定義加（＋）與乘（・）運算如下：

$$A+B=(A\setminus B)\cup(B\setminus A);$$
$$A\cdot B=A\cap B, A, B\in 2^S.$$

則它滿足

(1) $A+(B+C)=(A+B)+C, \forall A, B, C\in\wp(S);$

(2) 加法(+)運算的單位元素爲空集合 ϕ;

(3) $\forall A\in\wp(S), A+A=\phi$.所以, A 的加法反元素,就是 A 自己;.

(4) $A+B=B+A, \quad \forall A, B\in\wp(S);$

(5) $A\cdot(B\cdot C)=A\cap(B\cap C)=(A\cap B)\cap C=(A\cdot B)\cdot C$

(6) $A\cdot(B+C)=A\cdot B+A\cdot C, \quad \forall A, B\in\wp(S);$

$(B+C)\cdot A=B\cdot A+C\cdot A;$

又 $A\cdot B=A\cap B=B\cap A=B\cdot A$

所以,布爾環是交換環。

第三章 布 p 環

第一節 基本性質

（一）布 p 環的定義：若一個環 R 滿足 $x^p = x, \forall x \in R, p \geq 2$,我們稱之爲布 p 環。

（二）布 p 環的性質：

【引理 1】令 R 爲布 p 環且令 $r \in R$。若 $r^2 = 0$,則 $r = 0$。換言之,布 p 環中非零元素的平方非零。

【證明】因,

$$\begin{aligned} r &\overset{\text{布 } p \text{ 環}}{=} r^p \\ &= r^2 r^{p-2} \\ &\overset{r^2=0}{=} 0 \cdot r^{p-2} \\ &= 0 \end{aligned}$$

故得證。

【引理 2】令 R 爲布 p 環且令 $a \in R$。若 $a^2 = a$,則 $ax = xa, \forall x \in R$ 。

換言之,布 p 環中平方後不變的元素可跟任何元素交換。

【證明】分配律告訴我們

$$\begin{aligned} &(ax - axa)^2 \\ &= axax - axaxa - axaax + axaaxa \\ &= axax - axaxa - axa^2x + axa^2xa \end{aligned}$$

由假設條件 $a^2 = a$ 得知

$$\begin{aligned} &(ax - axa)^2 \\ &= axax - axaxa - axax + axaxa \\ &= 0 \\ &\overset{\text{引理 1}}{\Rightarrow} ax - axa = 0 \end{aligned}$$

因而我們有 $ax = axa$ 。

同理,

$$\begin{aligned} &(xa - axa)^2 = 0 \\ &\overset{\text{引理 1}}{\Rightarrow} xa - axa = 0 \end{aligned} \quad ;$$

我們有 $xa = axa$,故得證 $ax = axa = xa, \forall x \in R$ 。

【推論】布爾環是交換環。

【引理 3】令R爲布p環。則$y^{p-1}x = xy^{p-1}, \forall x, y \in R$。換言之,布$p$環中$p-1$次冪的元素可跟任何元素交換。

【證明】令$a = y^{p-1}$。則,

$$\begin{aligned} a^2 &= y^{2p-2} \\ &= y^p y^{p-2} \\ &\overset{\text{布 } p \text{ 環}}{=} yy^{p-2} \\ &= y^{p-1} \\ &= a \end{aligned}$$

$$\overset{\text{引理 } 2}{\Rightarrow} ax = xa, \forall x \in R$$

故得證。

【引理 4】令R爲布p環。則$(xy)^{p-1} = (yx)^{p-1}, \forall x, y \in R$。換言之,布$p$環中$p-1$次冪內部兩元素可互相交換。

【證明】因

$$\begin{aligned} (xy)^{p-1} &= xy(xy)^{p-2} \\ &\overset{\text{布}P\text{環}}{=} x^p y(xy)^{p-2} \\ &= x^{p-1}xy(xy)^{p-2} \\ &= x^{p-1}(xy)^{p-1} \\ &\overset{\text{引理}3}{=} (xy)^{p-1}x^{p-1} \end{aligned}$$

$$= \overbrace{(xyxy\cdots xy)}^{p-1\text{個}xy} xx^{p-2}$$

$$= x(yx)^{p-1} x^{p-2}$$

$$\overset{\text{引理3}}{=} (yx)^{p-1} xx^{p-2}$$

$$= (yx)^{p-1} x^{p-1}$$

$$= (yx)^{p-2} yxx^{p-1}$$

$$= (yx)^{p-2} yx^{p}$$

$$\overset{\text{布}P\text{環}}{=} (yx)^{p-2} yx$$

$$= (yx)$$

故得證。

【引理 5】令 R 爲布 p 環,其中 p 爲偶數。則 $2x = 0, \forall x \in R$ 。換言之,偶布 p 環中每一個元素的加法反元素就是它自己。

【證明】因

$$-x \overset{\text{布}p\text{環}}{=} (-x)^{p}$$

$$\overset{\text{偶}p}{=} x^{p}$$

$$\overset{\text{布}p\text{環}}{=} x$$

$$\Rightarrow 2x = x + x$$

$$= 0,$$

故得證。

第二節 布 3 環是交換環

【定理 1】布 3 環是交換環。

【證法 1】因 $\forall x, y \in R$

$$
\begin{aligned}
xy &\overset{\text{布 3 環}}{=} (xy)^3 \\
&= xy\,(xy)^2 \\
&\overset{\text{引理 3}}{=} x(xy)^2 y \\
&\overset{\text{結合律}}{=} x^2 yxy^2 \\
&\overset{\text{引理 3}}{=} yx^2 xy^2 \\
&= yx^3 y^2 \\
&\overset{\text{布 3 環}}{=} yxy^2 \\
&\overset{\text{引理 3}}{=} yy^2 x \\
&= y^3 x \\
&\overset{\text{布 3 環}}{=} yx
\end{aligned}
$$

故得證。

【證法 2】因 $\forall x, y \in R$

$$
\begin{aligned}
xy &\overset{\text{布 3 環}}{=} (xy)^3 \\
&= xy(xy)^2 \\
&\overset{\text{引理 4}}{=} xy(yx)^2 \\
&\overset{\text{結合律}}{=} x(y^2x)yx \\
&\overset{\text{引理 3}}{=} x(xy^2)yx \\
&\overset{\text{結合律}}{=} x^2y^3x \\
&\overset{\text{布 3 環}}{=} x^2yx \\
&\overset{\text{引理 3}}{=} yx^2x \\
&= yx^3 \\
&\overset{\text{布 3 環}}{=} yx
\end{aligned}
$$

故得證。

【注意】引理 3 才是上面證明的真正關鍵性質,此性質說：布 3 環中平方元素可跟任何元素交換。

第三節 布 4 環是交換環

【引理 6】在布 4 環 R 中,$(y^2+y)x = x(y^2+y), \forall x, y \in R$。換言之,布 4 環 R 中,平方加一次方的元素可跟任何元素交換。

【證明】令 $a = y^2 + y$。則

$$\begin{aligned} a^2 &= (y^2+y)^2 \\ &= y^4 + 2y^3 + y^2 \\ &\overset{\text{布4環,引理5}}{=} y + 0 + y^2 \\ &= y^2 + y \\ &= a \end{aligned}$$

$$\overset{\text{引理2}}{\Rightarrow} ax = xa, \forall x \in R$$

故得證。

【引理 7】在布 4 環 R 中,$(xy+yx)r = r(xy+yx), \forall x, y, r \in R$。換言之,布 4 環 R 中,兩元素相乘加交換相乘的元素可跟任何元素交換。

【證明】因

$$\begin{aligned} &(x+y)^2 + (x+y) \\ &= (x^2+x) + (y^2+y) + (xy+yx), \forall x, y, r \in R \end{aligned}$$

,故有

$$
\begin{aligned}
(x^2+x)r+(y^2+y)r+(xy+yx)r &\overset{\text{分配律}}{=} \left[(x^2+x)+(y^2+y)+(xy+yx)\right]r \\
&\overset{\text{上之因}}{=} \left[(x+y)^2+(x+y)\right]r \\
&\overset{\text{引理6}}{=} r\left[(x+y)^2+(x+y)\right] \\
&\overset{\text{上之因}}{=} r\left[(x^2+x)+(y^2+y)+(xy+yx)\right] \\
&\overset{\text{分配律}}{=} r(x^2+x)+r(y^2+y)+r(xy+yx)
\end{aligned}
$$

故得證。

【引理 8】在布 4 環 R 中, $y^2x = xy^2, \forall x, y \in R$ 。換言之,布 4 環 R 中平方的元素可跟任何元素交換。

【證明】在引理 7 中我們取 $r = y$ 得

$$
\begin{aligned}
&(xy+yx)y = y(xy+yx) \\
&\overset{\text{分配律}}{\Rightarrow} xy^2+yxy = yxy+y^2x \\
&\overset{\text{加法消去律}}{\Rightarrow} xy^2 = y^2x, \forall x, y \in R
\end{aligned}
$$

故得證。

【定理 2】布 4 環是交換環。

【證法 1】因布 4 環中平方元素可跟任何元素交換,所以 $\forall x, y \in R$

$$
\begin{aligned}
xy &\overset{\text{布 4 環}}{=} xy^4 \\
&\overset{\text{結合律}}{=} (xy^2)y^2 \\
&\overset{\text{引理 8}}{=} (y^2x)y^2 \\
&\overset{\text{結合律}}{=} y^2(xy^2) \\
&\overset{\text{引理 8}}{=} y^2(y^2x) \\
&\overset{\text{結合律}}{=} y^4x \\
&\overset{\text{布 4 環}}{=} yx
\end{aligned}
$$

故得證。

【證法 2】引理 6 告訴我們$\forall x, y \in R$

$$
\begin{aligned}
&(y^2+y)x = x(y^2+y) \\
&\overset{\text{分配律}}{\Rightarrow} y^2x + yx = xy^2 + xy \\
&\overset{\text{引理8,加法消去律}}{\Rightarrow} \quad yx = xy
\end{aligned}
$$

故得證。

【觀察 1】引理 8 是上面證明的真正關鍵性質,此性質說：布 4 環中平方元素可跟任何元素交換。這比起引理 3 所得到的「布 4 環中立方元素可跟任何元素交換」還更好。

【觀察 2】證法 1 的論證非常順暢,之所以如此乃在於 4 是偶數可分成兩半各得 2；而引理 8 所提供的性質配上布 4 環的性質,馬上得到所要的交換性,如下所示：

$$y \overset{\text{布4環}}{=} y^4 = y^2 \cdot y^2 \text{ 。}$$

一個元素 x 怎麼從 y 的左邊跑到 y 的右邊呢？只要看看上面等式最右側的 $y^2 \cdot y^2$ 即可了然於心。透過引理 8,元素 x 可跳過 y^2；連跳兩次就從左邊跑到右邊去了,就這麼簡單。

【觀察 3】所以當 p 是偶數時,布 p 環中的元素 y 可寫成：

$$y \overset{\text{布}p\text{環}}{=} y^p = y^{p/2} \cdot y^{p/2} \text{ 。}$$

只要可跳過 $y^{p/2}$,連跳兩次就從左邊跑到右邊；也就是說,可跳過 y 。

【引理 9】在偶布 p 環 R 中,若 $y^{p/2}x = xy^{p/2}, \forall x, y \in R$,則此布 p 環必定是交換環。

【證明】因 $\forall x, y \in R$

$$
\begin{aligned}
xy &= xy^{P} && \text{布}P\text{環} \\
&= \left(xy^{P/2}\right)y^{P/2} && \text{結合律} \\
&= \left(y^{P/2}x\right)y^{P/2} && \text{假設} \\
&= y^{P/2}\left(xy^{P/2}\right) && \text{結合律} \\
&= y^{P/2}\left(y^{P/2}x\right) && \text{假設} \\
&= y^{P}x && \text{結合律} \\
&= yx && \text{布}P\text{環}
\end{aligned}
$$

故得證。

第四章 布 5 環交換性的探討

【探討】布 5 環需加上什麼條件才有交換性？

【引理 10】令 R 爲布 5 環,若其中每一個元素都可以跟平方元素交換且每一個元素都可以跟立方元素交換,則此布 5 環必定是交換環。

【證明】（令 $C2$ 代表布 5 環中每一個元素都可以跟平方元素交換

$C3$ 代表布 5 環中每一個元素都可以跟立方元素交換）

我們有

$$\begin{aligned} xy &\overset{\text{布5環}}{=} xy^5 \\ &= \left(xy^3\right)y^2 \\ &\overset{C3}{=} \left(y^3x\right)y^2 \\ &\overset{\text{結合律}}{=} y^3\left(xy^2\right) \\ &\overset{C2}{=} y^3\left(y^2x\right) \\ &\overset{\text{結合律}}{=} y^5x \\ &\overset{\text{布5環}}{=} yx \end{aligned}$$

故得證。

【引理 11】令R爲布 5 環,若其中每一個元素都可以跟立方元素交換,則此布 5 環必定是交換環。

【證明】我們有

$$\begin{aligned}
xy &\overset{\text{布5環}}{=} (xy)^5 \\
&= xy(xy)^4 \\
&\overset{\text{引理 3}}{=} x(xy)^4 y \\
&= x^2(yx)^3 y^2 \\
&\overset{C3}{=} x^2 y^2 (yx)^3 \\
&= x^2 y^3 (xy)^2 x \\
&\overset{C3}{=} y^3 x^2 (xy)^2 x \\
&= y^3 x^3 (yx)^2 \\
&\overset{C3}{=} x^3 y^3 (yx)^2 \\
&= x^3 y^4 xyx \\
&\overset{\text{引理 3}}{=} y^4 x^3 xyx \\
&= y^4 (x^4 y)x \\
&\overset{\text{引理 3}}{=} y^4 (yx^4)x \\
&= y^5 x^5 \\
&\overset{\text{布5環}}{=} yx
\end{aligned}$$

故得證。

【注意】若布 5 環中每一個元素都可以跟立方元素交換,則此布 5 環必定是交換環。

參考文獻

[1] *Herstein,I.N.: Abstract Algebra,John Wiley & Son,Inc.,Third Edition, 1999.*

[2] *Agrawal, Manindra/Kayal, Neeraj/Saxena, Nitin： "PRIME is in P," Annals of Math 160（2004）,781-793.*

http：//www.cse.iitk.ac.in/news/primality.html

[3] *Apostol, Tom M.： Introduction to Analytic Number Theory, UTM, Springer-Verlag, New york, First Edition, 1976, Corr. Fifth Printing, 1998.*

[4] *Hardy,G./Wright E.： An Introduction to the Theory of Numbers,Fifth Edition, Oxford University Press,1979.*

[5] *Hardy,G.H.：A Course of Pure Mathematics, Cambridge Mathematical Library,1993（First published in 1908）.*

[6] *Hardy,G.H.：A Mathematician’s Apology, Cambridge University Press, London,1940.摘要見網頁 http://en.wikipedia.org/wiki/A_Mathematician%27s_ Apology*

[7] *Ireland, Kenneth F./Rosen, Michael I.: Michael I.: A Classical Introduction to Modern Number Theory, Volume 84 of Graduate Texts in Mathematics,Springer- Verlag,New York,Second Edition, 1990,Corr.Fifth Printing,1998.*

[8] *質數網頁 http://www.utm.edu/research/primes/largest.html*

[9] *沈淵源:密碼學之旅 全華圖書有限公司,2006.*