第八章　群和环

第十九节 环与域(2)

定理2 设 <A,+,·> 是无零因子环，当且仅当 运算 · 满足可消去性。

证明： **充分性** 设环<A,+,·>中 · 满足可消去性。

任取 $a,b\in R$，设有 $a\cdot b=0$ （往证$a=0\vee b=0$）（反证法）

(1) 假设 $a\neq 0$，因 $a\cdot 0=0$，于是 $a\cdot b=a\cdot 0$，由可消去性得 $b=0$；

(2) 假设 $b\neq 0$，因 $0\cdot b=0$，于是 $a\cdot b=0\cdot b$，由可消去性得 $a=0$ 。

由 $a\cdot b=0$ 推出 $a=0\vee b=0$ ，

因此<R,+,·>中无零因子。

定理2

设$<R,+,\cdot>$ 是无零因子环，当且仅当 运算 · 满足可消去性。

证明：必要性 设$<R,+,\cdot>$ 是无零因子环，

任取 $a,b,c\in R$，a不是零元且有 $a\cdot b=a\cdot c$

(往证$b=c$)

由 $a\cdot b=a\cdot c$，于是 $a\cdot b-a\cdot c=0$，于是 $a\cdot(b-c)=0$。

因$<R,+,\cdot>$是无零因子环，a不是零元，所以

$b-c=0$

即 $b+(-c)=0$，于是 $b=-(-c)=c$ 。

由 $a\cdot b=a\cdot c$ 推出 $b=c$，所以 · 满足可消去性。

定理3 设<A,+,·>是域，则 A 中无零因子。

证明： 因 <A-{0},·> 是交换群，所以对任何 $a \in A \wedge a \neq 0$，a 均是可消去元，即 · 运算在 A 中满足可消去性，由 定理2 知，它无零因子。

比较 整环 与 域 的差别：

整环

(1) <A,+> 是交换群；

(2) <A,·>是可交换独异点；

(3) 无零因子；

(4) · 对 + 可分配。

域

(1) <A,+> 是交换群；

(2) <A-{0},·>是交换群；

<A,·>是可交换独异点；

域中亦无零因子；

(4) · 对 + 可分配。

(3) <A-{0},·>是交换群；

对任意 $a\in A\wedge a\neq 0$，均有$a^{-1}\in A$；

定理4 域 必是 整环。

证明：因为 域 是 可交换的含幺环，又无零因子，所以域是整环。

整环 未必 是域。

例：<I,+, · > 是整环，但不是域。

因为对 · 运算，除 1 外的任何整数均不可逆 (1/n不是整数)，所以 <I-{0}, · > 不是群。

定理5 有限整环 必是 域 。

证明：设$<R,+,\cdot>$是有限整环，

令 $R=\{a_1, a_2, a_3, \dots, a_n\}$。 任取$a_i \in R \wedge a_i \neq 0$，

(往证 a_i 可逆)，

构造集合 $a_iR=\{a_i \cdot a_j \mid a_j \in R\}$ (类似左陪集)

(1) 先证 $a_iR=R$

对任意元素 $a_i \cdot a_j \in a_iR$，由$<R,\cdot>$封闭，于是 $a_i \cdot a_j \in R$，即 $a_iR \subseteq R$。

而 a_iR 中没有两个元素相同，(假设 a_iR 中有两个元素相同，设有 $a_i \cdot a_j = a_i \cdot a_k$ $(a_j, a_k \in R)$ $a_i \neq 0$，因R中无零因子，满足可消去性，于是 $a_j = a_k$, 矛盾。)

所以 $|a_iR|=|R|$，于是 $a_iR=R$。

定理5 有限整环必是域。

证明：(2) 再证 a_i 可逆

因为 <R,+, ·> 是含幺可交换环，于是 1∈R，由 $a_iR=R$，于是 $1\in a_iR$。所以必有 $a_k\in R$，使得 $a_i\cdot a_k=1$，又 · 可交换，$a_k\cdot a_i=1$，于是 $a_i^{-1}=a_k$， 即 R 中除 0 外均可逆，所以 <R-{0}, ·> 是交换群。因此 <R,+, ·> 是域。

第十九节 结束