Exercise

Chapter 1. 初級 Group 的性質

(1) 對任意正整數 n, 我們令 $\mathbb{Z}/n\mathbb{Z}$ 表示集合 $\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ 並定義其中的兩種運算 $\oplus, \odot$. 其定義分別如下: 為對任意 $\overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z}$, 若 $a+b$ 和 $a \cdot b$ 除以 n 的餘數分別為 r 和 s, 則令 $\overline{a} \oplus \overline{b} = \overline{r}$ 以及 $\overline{a} \odot \overline{b} = \overline{s}$.

- (a) 試問 $\mathbb{Z}/5\mathbb{Z}$ 在 $\oplus$ 的運算之下是否為一個 group? 其 identity 為何?
- (b) 試問 $\mathbb{Z}/5\mathbb{Z}$ 在 $\odot$ 的運算之下是否為一個 group? 若不是group, 請找到 $\mathbb{Z}/5\mathbb{Z}$ 最大的子集合使其在 $\odot$ 的運算下是一個 group.
- (c) 試問 $\mathbb{Z}/6\mathbb{Z}$ 在 $\oplus$ 的運算之下是否為一個 group? 其 identity 為何?
- (d) 試問 $\mathbb{Z}/6\mathbb{Z}$ 在 $\odot$ 的運算之下是否為一個 group? 若不是 group, 請找到 $\mathbb{Z}/6\mathbb{Z}$ 最大的子集合使其在 $\odot$ 的運算下是一個 group.

(2) 對任意兩個有理數 $a, b \in \mathbb{Q}$, 我們定義一個新的運算 $a * b = a + b + ab$.

- (a) 試問 $\mathbb{Q}$ 在 $*$ 這一個運算下是否是 closed (封閉性)?
- (b) 試證對任意 $a, b, c \in \mathbb{Q}$ 皆有 $a * (b * c) = (a * b) * c$.
- (c) 試找到 $e \in \mathbb{Q}$ 滿足對任意的 $a \in \mathbb{Q}$ 皆有 $e * a = a * e = a$.
- (d) 試找到 $\mathbb{Q}$ 中最大的子集合使其在 $*$ 的運算之下是一個 group.

(3) 假設 S 是一個集合且 $*$ 是 S 中的一個運算滿足:

(GP1): 若 $a, b \in S$ 則 $a * b \in S$.

(GP2): 若 $a, b, c \in S$ 則 $(a * b) * c = a * (b * c)$.

(GP3'): 在 S 中存在一個元素 e 使得 S 中所有元素 a 都有 $e * a = a$.

(GP4'): 對 S 任一元素 a 都可在 S 中找到某一元素 a' 使得 $a' * a = e$.

- (a) 試證明若 $a' * a = e$, 則 $a * a' = e$.
- (b) 試證明對任意 $a \in S$ 皆有 $a * e = a$.

(附註:由以上兩點得知 S 在 $*$ 的運算之下是一個 group.)

(4) 以下是有關 abelian group 一些簡單的性質:

   (a) 假設 G 是一個 abelian group, 試利用數學歸納法證明對任意 $a, b \in G$ 皆有 $(ab)^n = a^n b^n$, 其中 n 是任意的正整數.

   (b) 假設 G 是一個 group, 且對任意 $a \in G$ 皆滿足 $a^2 = e$, 試證明 G 一定是一個 abelian group.

(5) 假設 G 是一個 finite group. 以下是有關 finite group 一些簡單的性質:

   (a) 試證明對任意 $a \in G$, 存在一正整數 $n \in \mathbb{N}$ 使得 $a^n = e$.

   (b) 試證明存在一正整數 $n \in \mathbb{N}$ 使得對任意 $a \in G$ 皆有 $a^n = e$.

(6) 試證明所有 order (即元素個數) 為 $2, 3, 4, 5$ 的 finite group 皆為 abelian group.

(7) 設 G 是一個 group. $H_1, \ldots, H_n, \ldots$ 是 G 的 subgroups.

(a) 試證 $\bigcap_{i=1}^{\infty} H_i$ 是 G 的一個 subgroup.

(b) 若假設 $H_1 \subseteq H_2 \subseteq \cdots \subseteq H_{n-1} \subseteq H_n \subseteq H_{n+1} \subseteq \cdots$, 試證明 $\bigcup_{i=1}^{\infty} H_i$ 是 G 的一個 subgroup.

(8) 設 G 是一個 group. 給定 $a \in G$, 令 $C(a)$ 為 a 在 G 的 centralizer. 若 $Z(G)$ 是 G 的 center, 試證

$$Z(G) = \bigcap_{a \in G} C(a).$$

(9) 我們知道當 G 是 abelian group 時, 考慮 $C(a)$ 和 $Z(G)$ 並不會讓我們得到什麼有趣的 subgroup. 以下我們介紹一些當 G 是 abelian group 時可以考慮的一些 subgroup. 要注意以下這些例子在 abelian group 時才可保證是 subgroup, 在一般的情形並不一定會是 subgroup.

(a) 若 G 是一個 abelian group, 考慮集合

$$H = \{a \in G \mid a^2 = e\}.$$

試証 H 是 G 的一個 subgroup.

(b) 若 G 是一個 abelian group, 對任意 $n \in \mathbb{N}$, 考慮集合

$$A_n = \{a^n \mid a \in G\}.$$

試証 A_n 是 G 的一個 subgroup.

(c) 若 G 是一個 abelian group, 考慮集合

$$F = \{a \in G \mid 存在\ n \in \mathbb{N}\ 使得\ a^n = e\}.$$

試証 F 是 G 的一個 subgroup.

(d) 若 G 是一個 abelian group, 且 H_1, H_2 是 G 的 subgroups. 考慮集合

$$H_1H_2 = \{ab \mid a \in H_1,\ b \in H_2\}.$$

試証 H_1H_2 是 G 的一個 subgroup.

(10) 以下是有關 cyclic group 的簡單性質.

(a) 假設 G 是一個 cyclic group. 試證明 G 是一個 abelian group.

(b) 假設 G 是一個 cyclic group. 試證明 G 所有的 subgroup 都是 cyclic group.

Chapter 2. 中級 Group 的性質

(1) 設 G 是一個 group 且 H 為其 subgroup. 我們利用 H 對 G 中元素定兩種 relation. 第一種 relation 以 "$\sim$" 表示, 是如講義中所定: 對任意 $a, b \in G$ 我們定義 $a \approx b$ 若且唯若 $a^{-1} \cdot b \in H$. 第二種 relation 以 "$\approx$" 表示: 定義 $a \approx b$ 若且唯若 $b \cdot a^{-1} \in H$.

(a) 試證明 $\approx$ 是 G 中的一個 equivalent relation.

(b) 給定 $a \in G$ 試證明 $b \approx a$ 若且唯若 $b \in H \cdot a = \{h \cdot a \mid h \in H\}$.

(c) 一般來說 $\approx$ 和 $\sim$ 是不同的分類. 試證若 H 滿足對任意 $g \in G$, 皆有 $g \cdot H \cdot g^{-1} = H$, 則 $\approx$ 和 $\sim$ 是同樣的分類: 也就是說 $a \approx b$ 若且唯若 $a \sim b$.

(d) 試證若 $\approx$ 和 $\sim$ 是同樣的分類則 H 滿足對任意 $g \in G$, 皆有 $g \cdot H \cdot g^{-1} = H$.

(e) 假設 G/H 表示在 $\sim$ 分類下其 equivalent classes 所成的集合 (一般稱為 left cosets of H in G) 而 $H \backslash G$ 表示在 $\approx$ 分類下其 equivalent classes 所成的集合 (一般稱為 right cosets of H in G). 試證明 G/H 和 $H \backslash G$ 間存在一個一對一且映成的函數.

(2) 假設 G 是一個 cyclic group of order n 且 $G = \langle a \rangle$. 試證 $G = \langle b \rangle$ 若且唯若存在 $m \in \mathbb{N}$ 滿足 $\gcd(m, n) = 1$ 使得 $b = a^m$.

(3) 假設 G 是一個 abelian group of order n 且存在 $a, b \in G$ 滿足 $a \neq b$ 及 $\mathrm{ord}(a) = \mathrm{ord}(b) = 2$. 試證明 $4 \mid n$.

(4) 假設 G 是一個 abelian group of order n 且 $G = \{a_1, a_2, \ldots, a_n\}$. 令 $g = a_1 \cdot a_2 \cdots a_n$.

(a) 假設 G 中沒有元素滿足 $b \neq e$ 且 $b^2 = e$, 試證 $g = e$.

(b) 假設 $b \in G$ 是 G 中唯一的一個元素滿足 $b \neq e$ 且 $b^2 = e$, 試證 $g = b$.

(c) 假設 G 中有多於一個以上的元素滿足 $b \neq e$ 且 $b^2 = e$, 試證 $g = e$.

(5) 對任意整數 $n > 1$, 我們令 $(\mathbb{Z}/n\mathbb{Z})^* = \{\overline{m} \mid 1 \leq m \leq n-1, \gcd(m, n) = 1\}$ 並定義其中的運算 "$\cdot$" 如下: 為對任意 $\overline{a}, \overline{b} \in (\mathbb{Z}/n\mathbb{Z})^*$, 若 $a \cdot b$ 除以 n 的餘數分別為 r, 則令 $\overline{a} \cdot \overline{b} = \overline{r}$.

(a) 試證明 $(\mathbb{Z}/n\mathbb{Z})^*$ 是一個 group.

(b) 令 ϕ 表示為 Euler ϕ-function. 即對任意正整數 n, $\phi(n)$ 表示所有介於 1 和 n 之間且與 n 互質的整數的個數. 試證明 Euler 定理: 若 $a \in \mathbb{N}$ 且 $\gcd(a, n) = 1$, 則 $a^{\phi(n)} \equiv 1 \pmod{n}$ (即 $a^{\phi(n)}$ 除以 n 的餘數為 1).

(c) 試證明 Wilson 定理: 若 p 是一個質數, 則 $(p-1)! \equiv -1 \pmod{p}$ (即 $(p-1)!$ 除以 p 的餘數為 $p-1$).

(6) 假設 G 是一個 abelian group, $a, b \in G$. 其中 $\mathrm{ord}(a) = m$, $\mathrm{ord}(b) = n$ 且 $\gcd(m, n) = 1$. 試證明 $\mathrm{ord}(a \cdot b) = m \times n$.

---

19 October, 2006

(7) 設 G 是一個 group 且 M, N 都是 G 的 normal subgroup.
   (a) 試證明 $M \cap N$ 是 G 的一個 normal subgroup.
   (b) 若令 $MN = \{m \cdot n \mid m \in M, n \in N\}$, 試證 MN 是 G 的一個 normal subgroup.
   (c) 假設 $M \cap N = \{e\}$, 試證明對任意 $a \in M$, $b \in N$ 皆有 $a \cdot b = b \cdot a$.

(8) 設 G 是一個 group. H 是 G 的一個 subgroup. 考慮

$$N(H) = \{a \in G \mid a^{-1}Ha = H\}.$$

   (a) 試證 $N(H)$ 是 G 的一個 subgroup.
   (b) 試證明 H 是 $N(H)$ 的一個 normal subgroup.
   (c) 假設 K 是 G 的一個 subgroup 使得 H 是 K 的 normal subgroup. 試證明 $K \subseteq N(H)$. (通常我們稱 $N(H)$ 是 H 的 *normalizer*, 它是 G 中使得 H 在其中會 normal 的最大的 subgroup.)

(9) 設 G 是一個 group 且 N 是 G 的一個 normal subgroup. 假設 $\mathcal{M}$ 是 G/N 的一個 subgroup. 令 $M = \{a \in G \mid \overline{a} \in \mathcal{M}\}$.
   (a) 試證明 M 是 G 的一個 subgroup.
   (b) 試證明 $\mathcal{M}$ 是 G/N 的一個 normal subgroup 若且唯若 M 是 G 的一個 normal subgroup.

(10) 設 G 是一個 group 且 N 是 G 的一個 normal subgroup.
   (a) 試證明若 G 是一個 cyclic group 則 G/N 也是一個 cyclic group.
   (b) 試證明 G/N 是一個 abelian group 若且唯若對任意 $a, b \in G$ 皆滿足 $aba^{-1}b^{-1} \in N$.

(11) 設 G 是一個 group 且 $Z(G) = \{a \in G \mid ag = ga,\ \forall g \in G\}$ 為其 center.
   (a) 試證明 $Z(G)$ 是 G 的一個 normal subgroup.
   (b) 試證明若 $G/Z(G)$ 是一個 cyclic group, 則 G 是一個 abelain group.

(12) 假設 $\phi : G \to G'$ 是一個 onto (映成) 的 group homomorphism.
   (a) 假設 G 是一個 abelain group. 試證 G' 也是一個 abelian group.
   (b) 假設 N 是 G 的一個 normal subgroup. 試證 $\phi(N)$ 是 G' 的一個 normal subgroup.

26 October, 2006

(13) 令 G 為一個 group 且 N 為其 normal subgroup. 考慮函數 $\pi : G \to G/N$ 定義為 $\pi(a) = \overline{a}, \forall\, a \in G$.
  (a) 試證明 π 是一個 group homomorphism.
  (b) 試求 $\mathrm{im}(\pi)$.
  (c) 試求 $\ker(\pi)$.

(14) 假設 $\phi : G_1 \to G_2$ 以及 $\psi : G_2 \to G_3$, 都是 group homomorphism.
  (a) 試證明 $\psi \circ \phi : G_1 \to G_3$ 也是一個 group homomorphism.
  (b) 試證明 若 ϕ 是 1-1 且 onto, 則 $\phi^{-1} : G_2 \to G_1$ 也是一個 group homomorphism.
  (c) 試說明 groups 之間 isomorphic 的關係是一個 equivalent relation.

(15) 假設 G_1 和 G_2 都是 cyclic groups.
  (a) 若 G_1 是一個 finite group. 試證明 G_1 和 G_2 是 isomorphic 若且唯若 $|G_1| = |G_2|$.
  (b) 若 G_1 有無窮多個元素. 試證明 G_1 和 G_2 是 isomorphic 若且唯若 G_2 有無窮多個元素.

(16) 假設 G 是一個 abelian group. 對任意的正整數 n, 考慮函數 $\phi_n : G \to G$ 定義為 $\phi_n(a) = a^n$. 令 $G_n = \{a \in G \mid a^n = e\}$.
  (a) 試證明 ϕ_n 是一個 group homomorphism.
  (b) 試證明 G_n 是 G 的一個 subgroup 且 $\ker(\phi_n) = G_n$.
  (c) 若 $|G| = mn$, 試證明 $\mathrm{im}(\phi_n) \subseteq G_m$.
  (d) 若 $|G| = mn$ 且 $\gcd(m, n) = 1$. 試證明在 G/G_n 中若 $\overline{a}^n = \overline{e}$, 則 $a \in G_n$ (即 $\overline{a} = \overline{e}$).

(17) 令 G 為所有實係數的多項式, H 為所有常數項為 0 的實係數多項式 (即 $H = \{f(x) \in G \mid f(0) = 0\}$). 今在 G 中考慮一般多項式加法的結構.
  (a) 試證明 G 在加法的結構下是一個 group 且 H 為其 subgroup.
  (b) 試證明 G/H 和 $\mathbb{R}$ 在一般加法的結構下是 isomorphic.

(18) 令 G_1 和 G_2 為 groups 其運算分別用 $\cdot$ 和 $*$ 來表示並令 e_2 為 G_2 的 identity. 今考慮 $G = \{(a, b) \mid a \in G_1, b \in G_2\}$ 並考慮 G 中元素 (a, b) 和 (c, d) 之間的運算為 $(a, b)(c, d) = (a \cdot c, b * d)$.
  (a) 試證明 G 在此運算之下是一個 group.
  (b) 令 $N = \{(a, e_2) \mid a \in G_1\}$. 試證明 N 是 G 的 subgroup 且 N 和 G_1 是 isomorphic.
  (c) 試證明 N 是 G 的 normal subgroup 且 G/N 和 G_2 是 isomorphic.

(19) 考慮 $\mathbb{Z}$ 為整數在加法運算下之 group.

(a) 試證明

$$4\mathbb{Z}/12\mathbb{Z} \simeq 2\mathbb{Z}/6\mathbb{Z}.$$

(b) 假設 m, n 為正整數且 m, n 的最大公因數為 d, 最小公倍數為 l. 試證明

$$n\mathbb{Z}/l\mathbb{Z} \simeq d\mathbb{Z}/m\mathbb{Z}.$$

(20) 令 $G_1 = \mathbb{Z}$ 為整數在加法運算下之 group, $G_2 = \mathbb{Z}/6\mathbb{Z}$ 且 $\phi : G_1 \to G_2$ 是定義為 $\phi(n) = \overline{n}$ 的 group homomorphism. 考慮 $H_2 = 2\mathbb{Z}/6\mathbb{Z}$ 為 G_2 的 subgroup.

(a) 令 $H_1 = \{n \in \mathbb{Z} \mid \phi(n) \in H_2\}$. 試求 H_1.

(b) 考慮 $H_1' = 4\mathbb{Z}$. 試證明 $\phi(H_1') = H_2$.

(c) 試問 H_1 和 H_1' 是否相同? 若不同則與 correspondence theorem 的唯一性相違背, 其原因為何?

(21) 假設 $\phi : G_1 \to G_2$ 是一個 epimorphism (映成的 group homomorphism). 考慮

$$\begin{aligned}
\mathcal{S}_1 &= \{H_1 \subseteq G_1 \mid H_1 \text{ 是 } G_1 \text{ 的 subgroup 且 } \ker(\phi) \subseteq H_1\} \\
\mathcal{N}_1 &= \{N_1 \subseteq G_1 \mid H_1 \text{ 是 } G_1 \text{ 的 normal subgroup 且 } \ker(\phi) \subseteq N_1\} \\
\mathcal{S}_2 &= \{H_2 \subseteq G_2 \mid H_2 \text{ 是 } G_2 \text{ 的 subgroup}\} \\
\mathcal{N}_2 &= \{N_2 \subseteq G_2 \mid N_2 \text{ 是 } G_2 \text{ 的 normal subgroup}\}
\end{aligned}$$

(a) 試找到一個一對一且映成的函數將 $\mathcal{S}_1$ 映射到 $\mathcal{S}_2$.

(b) 試找到一個一對一且映成的函數將 $\mathcal{N}_1$ 映射到 $\mathcal{N}_2$.

Chapter 3. 一些常見的 Groups

(1) 令 G 是一個 cyclic group of order n 且令 ϕ 表示為 Euler ϕ-function. 即對任意正整數 m, $\phi(m)$ 表示所有介於 1 和 m 之間且與 m 互質的整數的個數.

  (a) 試證明若 $m \nmid n$ 則 G 中不存在 order 為 m 的元素.

  (b) 試證明若 $m \mid n$ 則 G 中存在 $\phi(m)$ 個 order 為 m 的元素.

  (c) 試證明 $n = \sum_{m|n} \phi(m)$.

(2) 假設 G 是一個 cyclic group of order n. 試證若 $m \in \mathbb{N}$ 且 $m \mid n$ 則存在唯一的 $H \subseteq G$ 是 G 的 subgroup 滿足 $|H| = m$.

(3) 若 $G_1, \ldots, G_n$ 是 groups, 考慮

$$G_1 \times \cdots \times G_n = \{(a_1, \ldots, a_n) \mid a_i \in G_i,\ \forall 1 \leq i \leq n\}.$$

對任意 $(a_1, \ldots, a_n), (b_1, \ldots, b_n) \in G_1 \times \cdots \times G_n$ 定義

$$(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) = (a_1 \cdot b_1, \ldots, a_n \cdot b_n).$$

試證明 $G_1 \times \cdots \times G_n$ 是一個 group.

(4) 若 G_1, G_2 是 groups 試證明 $G_1 \times G_2 \simeq G_2 \times G_1$

(5) 若 G 是一個 group 令 $T = \{(g, g) \in G \times G \mid g \in G\}$.

  (a) 試證明 T 是 $G \times G$ 的一個 subgroup.

  (b) 試證明 $T \simeq G$.

  (c) 試證明 T 是 $G \times G$ 的一個 normal subgroup 若且唯若 G 是一個 abelian group.

(6) 假設 G 是一個 finite group 且 N_1, N_2 是 G 的 normal subgroups.

(a) 已知 $G = N_1N_2$. 試證若 $|G| = |N_1|\,|N_2|$ 則 $G \simeq N_1 \times N_2$.

(b) 已知 $N_1 \cap N_2 = \{e\}$. 試證若 $|G| = |N_1|\,|N_2|$ 則 $G \simeq N_1 \times N_2$.

(7) 假設 G 是一個 abelian group 且 $|G| = m \times n$ 其中 $\gcd(m, n) = 1$. 試證明 G 是一個 cyclic group 若且唯若存在 $a, b \in G$ 滿足 $\mathrm{ord}(a) = m$ 且 $\mathrm{ord}(b) = n$.

(8) 若 G_1, G_2, G_3 為 groups 其中 e_1, e_2, e_3 分別為其 identity. 令 $G = G_1 \times G_2 \times G_3$. 考慮 $N_1 = \{(a, e_2, e_3) \in G \mid a \in G_1\}$, $N_2 = \{(e_1, b, e_3) \in G \mid b \in G_2\}$ 以及 $N_3 = \{(e_1, e_2, c) \in G \mid c \in G_3\}$.

(a) 試證 N_1, N_2, N_3 皆為 G 的 normal subgroup 且 $G = N_1N_2N_3$.

(b) 試證明 $N_1 \cap N_2 = N_1 \cap N_3 = N_2 \cap N_3 = \{(e_1, e_2, e_3)\}$.

(c) 試證明 $N_1 \cap N_2N_3 = N_2 \cap N_1N_3 = N_3 \cap N_1N_2 = \{(e_1, e_2, e_3)\}$.

(d) 在一般的情況 (2) 和 (3)並不是等價的. 試判斷 (2) 和 (3) 的性質哪一個是較強的.

(9) 假設 G 是一個 group 且 N_1, N_2, N_3 為其 normal subgroups 滿足 $G = N_1N_2N_3$ 且

$$N_1 \cap N_2N_3 = N_2 \cap N_1N_3 = N_3 \cap N_1N_2 = \{e\}.$$

試證明 $G \simeq N_1 \times N_2 \times N_3$.

(10) 假設 G 是一個 group 且 N 為其 normal subgroup. 考慮 G/N 這一個 quotient group.

(a) 假設 $a \in G$ 且 $\mathrm{ord}(a) = p$, 其中 p 是一個質數. 試證 $\mathrm{ord}(\overline{a}) = p$ 若且唯若 $a \notin N$.

(b) 假設 $b \in G$ 且 $\gcd(\mathrm{ord}(b), |N|) = 1$. 試證明 $\mathrm{ord}(\overline{b}) = \mathrm{ord}(b)$.

(c) 假設 $c \in G$ 且 $\gcd(\mathrm{ord}(c), |N|) = d$. 試證明 $\frac{\mathrm{ord}(c)}{d} \mid \mathrm{ord}(\overline{c})$.

(11) 假設 G 是一個 finite abelian group 且 $|G| = p^n m$ 其中 p 是一個質數且 $p \nmid m$. 試證對任意的 $r \in \mathbb{N}$ 且 $1 \leq r \leq n$ 皆存在一個 G 的 subgroup P_r 滿足 $|P_r| = p^r$.

(12) 假設 G 是一個 finite abelian group 且 $|G| = m$, 對任意 $n \in \mathbb{N}$ 考慮 $G_n = \{a \in G \mid a^n = e\}$. 試證明 $G_n = \{e\}$ 若且唯若 $\gcd(m, n) = 1$.

(13) 假設 G 是一個 finite abelian group 且 $|G| = p_1^{n_1} \cdots p_r^{n_r}$ 其中這些 p_i 是相異的質數. 令 P_i 為 G 的 Sylow-p_i subgroup. 試證明 $G \simeq P_1 \times \cdots \times P_r$.

(14) 假設 G 是一個 finite abelian group 且 p 是一個質數. 試證明 G 是一個 p-group 若且唯若 G 的每一個 subgroup 都是 p-group.

(15) 假設 G 是一個 finite abelian group.

(a) 已知 M, N 是 G 的 subgroup 且 $G \simeq M \times N$. 又知 $a \in M$, $b \in N$ 分別是 M 和 N 中 order 最大的元素, 試證明 $a \cdot b$ 是 G 中 order 最大的元素.

(b) 假設 M 是一個 p-group 且 $\mathrm{ord}(a) = p^r$, 試證明對任意 $x \in M$ 皆滿足 $x^{p^r} = e$.

(c) 假設 $\alpha \in G$ 是 G 中 order 最大的元素且 $\mathrm{ord}(\alpha) = n$. 試證明對任意 $x \in G$ 皆滿足 $x^n = e$.

(16) 由 Lagrange's Theorem 我們知若 $|G| = n$, $a \in G$ 且 $\mathrm{ord}(a) = m$, 則 $m \mid n$. Lagrange's Theorem 的反向是不對的也就是說若 $|G| = n$ 且 $m \mid n$ 並不表示存在 $a \in G$ 使得 $\mathrm{ord}(a) = m$. 雖然我們知這對 cyclic group 是對的但對 abelian group 就不對了. 考慮

$$G = (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/25\mathbb{Z}).$$

(a) 你可以找到 $m \in \mathbb{N}$ 滿足 $m < 1800 = |G|$ 且 $m \mid 1800$ 但是找不到 $a \in G$ 使得 $\mathrm{ord}(a) = m$ 嗎?

(b) 試列出 G 中元素所有可能的 order.

(17) 若 G_1, G_2 皆為 finite abelian group 且 $|G_1| = |G_2|$. 已知 a, b 分別是 G_1, G_2 中 order 最大的元素且 $\mathrm{ord}(a) = \mathrm{ord}(b)$. 試問是否可得 $G_1 \simeq G_2$? 若是證明之, 否則請提出反例.

(18) 試列出所有 order 為 600 的 abelian groups 並在每一個 group 中列出一個 order 最大的元素及其 order.

(19) 若 S_1, S_2 皆為有限集合, 令 $A(S_i)$ 表示為所有 S_i 到 S_i 的一對一且映成的函數所成的 group. 試證明 $A(S_1) \simeq A(S_2)$ 若且唯若 $|S_1| = |S_2|$.

(20) 令 G 是一個 group. 一個 G 到 G 的 group isomorphism 稱為 G 的 automorphism. 考慮 $\mathrm{Aut}(G)$ 為所有 G 的 group automorphisms 所成的集合且考慮合成為其間的運算.

(a) 試證明 $\mathrm{Aut}(G)$ 是一個 group.

(b) 固定 $a \in G$, 考慮 $T_a : G \to G$, 定義為 $T_a(x) = a \cdot x \cdot a^{-1}$, $\forall x \in G$. 試證明 $T_a \in \mathrm{Aut}(G)$.

(c) 考慮函數 $\phi : G \to \mathrm{Aut}(G)$ 定義為 $\phi(a) = T_a$, $\forall a \in G$. 試證明 ϕ 是一個 group homomorphism 並求 ϕ 之 kernel.

(21) 將下列 permutations 寫成 disjoint cycles 的乘積並計算其 order.

(a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 3 & 4 & 6 & 5 & 7 \end{pmatrix}$

(b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{pmatrix}$

(c) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 1 & 4 & 2 & 7 & 6 & 9 & 8 & 5 \end{pmatrix}$

(d) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 5 & 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{pmatrix}$

(e) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 5 & 3 & 4 & 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 1 & 5 & 6 & 7 & 4 \end{pmatrix}$

(f) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 2 & 5 \end{pmatrix}^{-1}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 2 & 5 \end{pmatrix}$

(g) $(\,1\ \ 2\ \ 3\ \ 5\ \ 7\,)(\,2\ \ 4\ \ 7\ \ 6\,)$

(h) $(\,1\ \ 2\ \ 3\ \ 4\ \ 5\,)(\,1\ \ 2\ \ 3\ \ 4\ \ 6\,)(\,1\ \ 2\ \ 3\ \ 4\ \ 7\,)$

(i) $(\,1\ \ 2\ \ 3\,)(\,3\ \ 5\ \ 7\ \ 9\,)(\,1\ \ 2\ \ 3\,)^{-1}$

(j) $(\,1\ \ 2\ \ 3\,)^{-1}(\,3\ \ 5\ \ 7\ \ 9\,)(\,1\ \ 2\ \ 3\,)$

(22) 考慮在 S_n 中, 其中 $n \geq 7$

(a) 試證存在 $\sigma \in S_n$ 使得 $\sigma(1\ \ 2\ \ 3)\sigma^{-1} = (5\ \ 6\ \ 7)$.

(b) 試證明不可能存在 $\sigma \in S_n$ 使得 $\sigma(1\ \ 2\ \ 3)\sigma^{-1} = (1\ \ 2\ \ 4)(5\ \ 6\ \ 7)$.

(23) 假設 $\sigma, \tau \in S_n$ 且 $\sigma = \sigma_1 \cdots \sigma_r$ 和 $\tau = \tau_1 \cdots \tau_r$ 分別是它們的 disjoint cycles decomposition, 其中對任意 $i \in \{1, \ldots, r\}$, σ_i 和 τ_i 都是 m_i-cycle. 試證明存在 $\rho \in S_n$ 使得 $\tau = \rho\sigma\rho^{-1}$.

(24) 令 τ_1, τ_2, τ_3 是 S_n $(n \geq 3)$ 中的 2-cycles (不一定 disjoint 也不一定相異).

(a) 試找出 $\tau_1\tau_2$ 可能的 order.

(b) 試證明 $\tau_1\tau_2\tau_3$ 不可能是 S_n 中的 identity.

(c) 試找出 $\tau_1\tau_2\tau_3$ 可能的 order.

(25) 假設 $\sigma \in S_n$ 是一個 k-cycle. 試證明 $\sigma \in A_n$ 若且唯若 k 是奇數.

(26) 假設 $m < n$, 我們定一以下的函數 $\Phi : S_m \to S_n$ 其定義如下: 若 $\sigma \in S_m$, 則令 $\Phi(\sigma) \in S_n$ 滿足

$$\Phi(\sigma)(i) = \begin{cases} \sigma(i), & \text{if } 1 \leq i \leq m; \\ i, & \text{if } m < i \leq n. \end{cases}$$

(a) 試證明 Φ 是一個 monomorphism.

(b) 試證明對任意 $\sigma \in S_m$, $\sigma \in A_m$ 若且唯若 $\Phi(\sigma) \in A_n$.

(27) 試判斷下列哪些是 even permutation.

(a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 4 & 5 & 1 & 3 & 7 & 8 & 9 & 6 \end{pmatrix}$

(b) $(\,1\ \ 2\ \ 3\ \ 4\ \ 5\ \ 6\,)(\,7\ \ 8\ \ 9\,)$

(c) $(\,1\ \ 2\ \ 3\ \ 4\ \ 5\ \ 6\,)(\,1\ \ 2\ \ 3\ \ 4\ \ 5\ \ 7\,)$

(d) $(\,1\ \ 2\,)(\,1\ \ 2\ \ 3\,)(\,4\ \ 5\,)(\,5\ \ 6\ \ 8\,)(\,1\ \ 7\ \ 9\,)$

(e) 若 $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 1 & 2 & x & y & 7 & 8 & 9 & 6 \end{pmatrix}$ 是 even permutation, 試問 x, y 之值.

(28) 假設 H 是 S_n 的 subgroup 且 $H \not\subseteq A_n$. 試證明 H 必有偶數個元素且 $|H \cap A_n| = \frac{1}{2}|H|$.

(29) 考慮 $n \geq 5$.

(a) 試找出 $\sigma \in A_n$ 使得 $\sigma \cdot (1\ \ 2\ \ 3)\sigma^{-1} = (3\ \ 4\ \ 5)$.

(b) 若 $\sigma = (1\ \ 2)(3\ \ 4)$ 試找到一個 2-cycle τ 及一個 3-cycle ρ 使得 $\sigma\tau\sigma^{-1} \neq \tau$ 且 $\sigma\rho\sigma^{-1} \neq \rho$.

(c) 若 $\delta = (1\ \ 2)(3\ \ 4)$ 試找一個 $\gamma \in S_n$ 使得 $\delta\gamma\delta\gamma^{-1}$ 是一個 3-cycle.

(d) 若 $\delta = (1\ \ 2\ \ 3)(1\ \ 2\ \ 4)$ 試找一個 $\gamma \in A_n$ 使得 $\delta\gamma\delta\gamma^{-1}$ 是一個 3-cycle.

(e) 若 $\delta = (1\ \ 2\ \ 3)(1\ \ 4\ \ 5)$ 試找一個 $\gamma \in A_n$ 使得 $\delta^{-1}\gamma\delta\gamma^{-1}$ 是一個 3-cycle.

(30) 考慮 $n > 2$.

(a) 試證明若 n 是奇數, 則每一個 even permutation 都可以寫成 $n-1$ 個 2-cycle 的乘積而每個 odd permutation 可以寫成 $n-2$ 個 2-cycle 的乘積. 當 n 是偶數情況又如何？

(b) 試證明 A_n 中的元素都可以寫成一些 n-cycle 的乘積.

(c) 假設 σ 是一個 k-cycle. 試證明 σ^2 仍為一個 cycle 若且唯若 k 是奇數. 在更一般的情形, 即若 σ 是一個 k-cycle 且 σ^r 是一個 cycle, 能否得到 k 和 r 有何關係？

---

04 January, 2007

Chapter 4. 進階 Group 的性質

(1) 假設 $(G, S, *)$ 是一個 group action, $x \in S$, 我們定義
$$G_x = \{g \in G \mid g * x = x\}.$$
試證明若 $a \in G$, 則 $a \cdot G_x \cdot a^{-1} = G_{a*x}$.

(2) 假設 G 是一個 group, 令 $S = G$ 且對任意 $g \in G, s \in S$, 我們定義 $g * s = g \cdot s \cdot g^{-1}$. 考 慮 $(G, S, *)$ 這一個 group action.

(a) 試證明對任意 $s \in S$, $G_s = C(s) = \{g \in G \mid g \cdot s = s \cdot g\}$.

(b) 若 $a, b \in G$ 且存在 $g \in G$ 使得 $b = g \cdot a \cdot g^{-1}$, 我們就稱 b 和 a 在 G 中 *conjugate*. 在 G 中所有和 a conjugate 的元素所成的集合就稱為 a 的 *conjugacy class*. 若令 $[a] = \{g \cdot a \cdot g^{-1} \mid g \in G\}$ 表示 a 的 conjugacy class, 試證明當 G 是一個 finite group 時
$$|[a]| = \frac{|G|}{|C(a)|}.$$

(c) 試證明 $[a] = \{a\}$ 若且唯若 $a \in Z(G)$.

(d) 假設 G 是一個 finite group 且 $[a_1], \ldots, [a_z], \ldots, [a_m]$ 是 G 中所有相異的 conjugacy class, 其中 $Z(G) = \{a_1, \ldots, a_z\}$. 試證明以下之 “*class equation*”
$$|G| = z + \sum_{i=z+1}^{m} \frac{|G|}{|C(a_i)|}.$$

(e) 試利用 class equation 以及數學歸納法證明 Cauchy's Theorem.

(3) 以下我們探討 S_n 中的 conjugacy classes.

(a) 試找出 S_4 和 S_5 各有多少個相異 conjugacy classes. 並驗證其 class equation.

(b) 若共有 $p(n)$ 種方法(若僅是順序不同算相同方法)將 n 寫成一些正整數和. 試證明 S_n 中所有相異的 conjugacy classes 的個數等於 $p(n)$, 並證明 S_n 中所有相異的 conjugacy classes 的個數等於所有個數為 2^n 且不互相 isomorphic 的 abelian groups 的個數.

(c) 若 $\sigma \in S_n$ 是一個 m-cycle, 試計算在 S_n 中可以和 σ 交換的元素個數 (即 $|C(\sigma)|$).

(4) 假設 G 是一個 order 為 p^3 的 group (其中 p 為質數). 試證明 G 是 abelian 若且唯若 $|Z(G)| \geq p^2$.

(5) 以下是有關 p-group 的重要性質.

(a) 試證明 G 是一個 p-group 若且唯若 G 的每一個 subgroup 都是 p-group.

(b) 試證明若 G 是一個 p-group, 則對任意 $m \mid |G|$ 皆存在 G 的一個 normal subgroup N 滿足 $|N| = m$.

Chapter 5. 初級 **Ring** 的性質

(1) 假設 R 是一個 ring. 對任意 $a \in R$, 當 $n \in \mathbb{N}$ 時令

$$na = \underbrace{a + \cdots + a}_{n} \text{ 且 } (-n)a = -na.$$

(a) 試利用數學歸納法證明當 $m, n \in \mathbb{N}$ 時對任意 $a, b \in R$ 皆有

$$(ma) \cdot (nb) = (mn)(a \cdot b).$$

(b) 試證明當 $m, n \in \mathbb{Z}$ 時對任意 $a, b \in R$ 皆有

$$(ma) \cdot (nb) = (mn)(a \cdot b).$$

(2) 假設 R 是一個 ring.

(a) 若 $a \in R$ 滿足 $a^2 = a$, 試證明對任意 $b \in R$ 皆有

$$(b \cdot a - a \cdot b \cdot a)^2 = (a \cdot b - a \cdot b \cdot a)^2 = 0.$$

(b) 試證明若對任意 $a \in R$ 皆有 $a^2 = a$, 則 R 是一個 commutative ring.

(3) 假設 R 是一個 integral domain 且僅有有限多個元素.

(a) 試證明 R 是一個 field.

(b) 試證明存在一個質數 p 使得對任意 $a \in R$ 皆有 $pa = 0$.

(c) 利用 (b) 以及 Cauchy's Theorem 證明若 R 有 q 個元素, 則存在 $n \in \mathbb{N}$ 使得 $q = p^n$.

(4) 令 $p \in \mathbb{N}$ 是一個質數. $R \subseteq \mathbb{Q}$ 是有理數中寫成最簡分數時其分母不能被 p 整除的元素所成的集合, 亦即若 $m/n \in R$ 其中 $m, n \in \mathbb{Z}$ 且 $\gcd(m, n) = 1$, 則 $p \nmid n$.

(a) 試證在一般有理數的加法和乘法之下 R 是一個 ring.

(b) 試證明 R 是一個 integral domain.

(c) 試說明 R 不是一個 field 並找出 R 中所有的 unit.

(5) 令 $R = \{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{R}\}$ 試證明在一般矩陣的加法和乘法之下 R 是一個 field.

(6) 假設 R 是一個 ring with 1 且 $a, b \in R$ 滿足 $a \cdot b = 1$.

(a) 試證明若 a 不是 R 的 zero divisor, 則 a 是 R 中的 unit.

(b) 若 b 是 R 中唯一的元素滿足 $a \cdot b = 1$, 試證明 a 不是 R 的 zero divisor 因而得知 a 是 R 中的 unit.

(7) 假設 R 是一個 ring 且 $r, s \in R$. 下列哪些有關於 zero divisor 的敘述是對的?

(a) 若 r, s 都是 zero divisor, 則 $r + s$ 是 zero divisor.

(b) 若 r, s 都是 zero divisor, 則 $r \cdot s$ 是 zero divisor.

(c) 若 r, s 都不是 zero divisor, 則 $r + s$ 不是 zero divisor.

(d) 若 r, s 都不是 zero divisor, 則 $r \cdot s$ 不是 zero divisor.

(e) 若 r, s 中只要有一個不是 zero divisor, 則 $r \cdot s$ 和 $s \cdot r$ 中必有一個不是 zero divisor.

(f) 若 r, s 中只要有一個是 zero divisor, 則 $r \cdot s$ 和 $s \cdot r$ 中必有一個是 zero divisor.

(8) 假設 R 是一個 ring with 1 且 $r, s \in R$. 下列哪些有關於 unit 的敘述是對的?

(a) 若 r, s 都是 unit, 則 $r + s$ 是 unit.

(b) 若 r, s 都是 unit, 則 $r \cdot s$ 是 unit.

(c) 若 r, s 都不是 unit, 則 $r + s$ 不是 unit.

(d) 若 r, s 都不是 unit, 則 $r \cdot s$ 不是 unit.

(e) 若 r, s 中只要有一個是 unit, 則 $r \cdot s$ 和 $s \cdot r$ 都是 unit.

(f) 若 r, s 中只要有一個不是 unit, 則 $r \cdot s$ 和 $s \cdot r$ 都不是 unit.

(9) 假設 R 是一個 nontrivial ring. 令 $M_2(R) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in R\}$. 在 $M_2(R)$ 中我們考慮一般矩陣之加法及乘法.

(a) 若 $A, B, C \in M_2(R)$ 試證明 $(AB)C = A(BC)$ 以及

$$A(B + C) = AB + AC \quad \text{and} \quad (A + B)C = AC + BC.$$

(b) 不管 R 是否有 zero divisor 試在 $M_2(R)$ 中找到一個 zero divisor.

(c) 假設 R 沒有乘法的 identity. 試證明 $M_2(R)$ 也沒有乘法的 identity.

(d) 試證明 $T = \{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in R\}$ 是 $M_2(R)$ 的一個 subring.

(e) 假設 R 有乘法的 identity. 試證明 $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in T$ 是 T 的一個 unit 若且唯若 a, c 皆為 R 中的 unit.

(10) 令 $\mathbb{H} = \{a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \mid a, b, c, d \in \mathbb{R}\}$ 是 Hamilton quaternion ring. 若 $u = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \in \mathbb{H}$ 我們令 $\overline{u} = a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}$.

(a) 若 $u = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \in \mathbb{H}$ 試證明 $u\overline{u} = \overline{u}u = a^2 + b^2 + c^2 + d^2$

(b) 若 $u, v \in \mathbb{H}$ 試證明 $\overline{uv} = \overline{v}\,\overline{u}$.

(c) 假設 $(a_1 + b_1\mathbf{i} + c_1\mathbf{j} + d_1\mathbf{k})(a_2 + b_2\mathbf{i} + c_2\mathbf{j} + d_2\mathbf{k}) = a_3 + b_3\mathbf{i} + c_3\mathbf{j} + d_3\mathbf{k}$. 試證明 $(a_1^2 + b_1^2 + c_1^2 + d_1^2)(a_2^2 + b_2^2 + c_2^2 + d_2^2) = a_3^2 + b_3^2 + c_3^2 + d_3^2$.

Chapter 6. 中級 Ring 的性質

(1) 假設 R 是一個 ring, I 是 R 的 ideal 且 A 是 R 的 subring. 試證明 $I \cap A$ 是 A 的 ideal.

(2) 假設 R 是一個 ring, I 是 R 的 ideal 且 $a \in R$. 考慮

$$L_a(I) = \{x \in R \mid xa \in I\}.$$

(a) 試證明若 R 是一個 ring with 1 且 a 是 R 的 unit, 則 $L_a(I) = I$.

(b) 試證明若 R 是 commutative 則 $L_a(I)$ 是 R 的一個 ideal.

(c) 試說明當 R 不是 commutative 時, $L_a(I)$ 有可能不是 R 的一個 ideal.

(d) 試問若考慮 $I_a = \{x \in R \mid xa \in I \quad \text{or} \quad ax \in I\}$, 則當 R 不是 commutative 時, I_a 是否一定是 R 的一個 ideal?

(3) 假設 R 和 S 都是 ring. 考慮 R 和 S 的 direct sum

$$R \oplus S = \{(r, s) \mid r \in R, s \in S\}.$$

定義 $R \oplus S$ 中的加法和乘法為:

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2), \quad (r_1, s_1) \cdot (r_2, s_2) = (r_1 \cdot r_2, s_1 \cdot s_2).$$

(a) 試證明在此加法和乘法的定義之下 $R \oplus S$ 是一個 ring.

(b) 考慮 $R' = \{(r, 0) \mid r \in R\} \subseteq R \oplus S$ 和 $S' = \{(0, s) \mid s \in S\} \subseteq R \oplus S$. 試證明 R' 和 S' 皆為 $R \oplus S$ 的 ideal.

(4) 假設 R 是一個 ring. 在 $M_2(R)$ 中考慮

$$T = \{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in R\} \quad \text{and} \quad I = \{\begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} \mid a \in R\}.$$

試證明 I 是 T 的 ideal 但不是 $M_2(R)$ 的 ideal.

(5) 假設 R 是一個 ring with 1. 考慮 $M_2(R)$ 這個 ring. 對任意 $i, j \in \{1, 2\}$ 我們令 $\mathcal{E}_{ij} \in M_2(R)$ 表示第 (i, j) 位置是 1 其他位置是 0 的矩陣.

(a) 試證明對任意 $A = (a_{ij}) \in M_2(R)$ ($a_{ij} \in R$ 表示 A 這個矩陣第 (i, j) 個位置的元素), $i, j, k, l \in \{1, 2\}$ 皆有 $\mathcal{E}_{ij} A \mathcal{E}_{kl} = a_{jk} \mathcal{E}_{il}$.

(b) 假設 $\mathcal{I}$ 是 $M_2(R)$ 的一個 ideal. 考慮 $I = \{a_{11} \mid A = (a_{ij}) \in \mathcal{I}\}$. 試證明 I 是 R 的一個 ideal.

(c) 試證明 $\mathcal{I} = M_2(I) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in I\}$

(d) 試證明若 R 是一個 division ring 則 $M_2(R)$ 中的 ideal 只有 $\{\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\}$ 和 $M_2(R)$.

(6) 假設 R 是一個 ring 並考慮 $R \oplus R = \{(a,b) \mid a,b \in R\}$ 這個 ring.

(a) 令 $I = \{(a,0) \mid a \in R\}$ 試證明 I 是 $R \oplus R$ 的一個 ideal.

(b) 試證明 $(R \oplus R)/I \simeq R$.

(c) 若 R 是一個 division ring 試找出 $R \oplus R$ 中所有包含 I 的 ideal.

(7) 假設 $\phi : R \to R'$ 是一個 ring homomorphism.

(a) 令 $1_R, 1_{R'}$ 分別為 R 和 R' 乘法的 identity. 若 ϕ 是 onto 的試證明 $\phi(1_R) = 1_{R'}$.

(b) 試舉一個例子 ϕ 不是 onto 但 $\phi(1_R) \neq 1_{R'}$.

(c) 若已知 R 是一個 division ring 且存在 $a \in R$ 使得 $\phi(a) \neq 0$. 試證明 ϕ 是一對一.

(8) 令 $R = \{a + b\sqrt{2} \mid a,b \in \mathbb{Z}\}$, $R' = \{\begin{pmatrix} c & 2d \\ d & c \end{pmatrix} \mid c,d \in \mathbb{Z}\}$. 考慮 R 中的加法和乘法為一般實數的加法與乘法, 而 R' 中的加法和乘法為一般矩陣的加法與乘法.

(a) 試證明 R 為一個 ring 且 $I = \{2a + b\sqrt{2} \mid a,b \in \mathbb{Z}\}$ 是 R 的一個 ideal.

(b) 試證明 R' 是一個 ring 且找到一個 ring isomorphism $\phi : R' \to R$.

(c) 由 (b) 中的 ϕ, 試寫下 $\phi^{-1}(I)$. 並驗證其確為 R' 的 ideal.

(9) 假設 R 是一個 ring. 令 $R' = \{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a,b,c \in R\}$, 已知在一般矩陣的運算之下 R' 是一個 ring. 今考慮

$$I = \{\begin{pmatrix} 0 & d \\ 0 & 0 \end{pmatrix} \mid d \in R\} \quad \text{and} \quad I' = \{\begin{pmatrix} e & 0 \\ 0 & f \end{pmatrix} \mid e,f \in R\}.$$

(a) 試證明 I 是 R' 的 一個 ideal 且 $R'/I \simeq R \oplus R$.

(b) 考慮 $\phi : R' \to R$ 定義為 $\phi(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}) = b$. 試問 ϕ 是否為一個 group homomorphism? 是否為一個 ring homomorphism?

(c) 試證明看成是 group R'/I' 和 R 是 isomorphic; 並檢驗 I' 不是 R' 的 ideal (所以 R'/I' 不是一個 ring).

(d) 試找到 R' 中的一個 ideal J 滿足 $R'/J \simeq R$ (as a ring).

(10) 假設 R 是一個 ring, I, J, 皆為 R 的 ideal.

(a) 試證明 $R/(I \cap J)$ 會和 $R/I \oplus R/J$ 的一個 subring isomorphic.

(b) 試證明若 $m, n \in \mathbb{N}$ 滿足 $\gcd(m,n) = 1$ 則

$$\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/mn\mathbb{Z}.$$

(c) 試證明中國剩餘定理: 若 $m, n \in \mathbb{N}$ 滿足 $\gcd(m,n) = 1$, 則給定任意的 $a, b \in \mathbb{Z}$ 皆存在一個整數 x 滿足 $x \equiv a \pmod{m}$ 且 $x \equiv b \pmod{n}$.

(11) 若 R 是 commutative ring with 1 且 $a \in R$. 試證明若 I 是 R 的 ideal 且 $a \in I$, 則 $(a) \subseteq I$.

(12) 令 $\mathbb{Z}[\mathbf{i}] = \{a + b\mathbf{i} \mid a, b \in \mathbb{Z}\}$ 為 $\mathbb{C}$ 的 subring (其中 $\mathbf{i}^2 = -1$).

(a) 試證明在 $\mathbb{Z}[\mathbf{i}]$ 中若 I 是一個 ideal 且 $a + b\mathbf{i} \in I$, 則 $a^2 + b^2 \in I$.

(b) 試寫下在 $\mathbb{Z}[\mathbf{i}]$ 中 (5) 這個 principle ideal 中元素的形式並推得 $2-\mathbf{i} \notin (5)$.

(c) 試證明 $\mathbb{Z}[\mathbf{i}]$ 中 (5) 不是一個 prime ideal.

(d) 試證明若 I 是 $\mathbb{Z}[\mathbf{i}]$ 中的一個 ideal 且 $(3) \subsetneq I$, 則必存在 $n \in \mathbb{Z}$ 滿足 $n \in I$ 且 $3 \nmid n$.

(e) 試證明在 $\mathbb{Z}[\mathbf{i}]$ 中 (3) 是一個 maximal ideal.

(13) 假設 $\phi : \mathbb{Z}[\mathbf{i}] \to \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$ 是一個 ring epimorphism.

(a) 試證明 $\phi(1) = (\overline{1}, \overline{1})$ 且 $\phi(-1) = (\overline{4}, \overline{4})$.

(b) 試利用 $\mathbf{i}^2 = -1$ 證明 $\phi(\mathbf{i}) = (u, v)$ 其中 $u, v \in \{\overline{2}, \overline{3}\}$.

(c) 若假設 $\phi(\mathbf{i}) = (\overline{2}, \overline{3})$ 試說明 $\phi(a + b\mathbf{i}) = (\overline{a + 2b}, \overline{a + 3b})$ 並驗證如此定義之 ϕ 確為 $\mathbb{Z}[\mathbf{i}]$ 到 $\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$ 的一個 ring epimorphism.

(d) 試證明 $\mathbb{Z}[\mathbf{i}]/(5) \simeq \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$.

(e) 試說明 (5) 不是 $\mathbb{Z}[\mathbf{i}]$ 的 prime ideal.

(f) 若 $\phi(\mathbf{i}) = (\overline{3}, \overline{2})$, 是否能定出一個 $\mathbb{Z}[\mathbf{i}]$ 到 $\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$ 的一個 ring epimorphism? 若能請寫下其形式並求其 kernel.

(g) 若 $\phi(\mathbf{i}) = (\overline{2}, \overline{2})$, 是否能定出一個 $\mathbb{Z}[\mathbf{i}]$ 到 $\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$ 的一個 ring epimorphism?

(14) 假設 $\phi : \mathbb{Z}[\mathbf{i}] \to \mathbb{Z}/5\mathbb{Z}$ 是一個 ring epimorphism.

(a) 試證明 $\phi(\mathbf{i}) = \overline{2}$ 或 $\phi(\mathbf{i}) = \overline{3}$.

(b) 試說明若 $\phi(\mathbf{i}) = \overline{2}$ 時確實能定出一個 $\mathbb{Z}[\mathbf{i}]$ 到 $\mathbb{Z}/5\mathbb{Z}$ 的一個 ring epimorphism. 請寫下其形式並證明 $\ker(\phi) = (2 - \mathbf{i})$.

(c) 試說明 $(2 - \mathbf{i})$ 是 $\mathbb{Z}[\mathbf{i}]$ 的一個 maximal ideal.

(d) 若 $\phi(\mathbf{i}) = \overline{3}$, 是否能定出一個 $\mathbb{Z}[\mathbf{i}]$ 到 $\mathbb{Z}/5\mathbb{Z}$ 的一個 ring epimorphism. 請寫下其形式並求其 kernel.

(15) 已知在 $\mathbb{Z}[\mathbf{i}]$ 中 (3) 是一個 maximal ideal.

(a) 試找到一個 $\mathbb{Z}[\mathbf{i}]$ 到 $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ 加法的 group epimorphism.

(b) 說明 $\mathbb{Z}[\mathbf{i}]/(3)$ 是一個有 9 個元素的 field.

(c) 試說明 $\mathbb{Z}[\mathbf{i}]/(3)$ 看成是 加法的 group 時可以和 $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ isomorphic 但不能和 $\mathbb{Z}/9\mathbb{Z}$ isomorphic.

(d) 試說明 $\mathbb{Z}[\mathbf{i}]/(3)$ 看成是 ring 時不可以和 $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ isomorphic 也不可以和 $\mathbb{Z}/9\mathbb{Z}$ isomorphic.

(e) 試說明不可能找到一個 $\mathbb{Z}[\mathbf{i}]$ 到 $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ 的一個 ring epimorphism 也不可能找到一個 $\mathbb{Z}[\mathbf{i}]$ 到 $\mathbb{Z}/9\mathbb{Z}$ 的一個 ring epimorphism..

---

29 March, 2007

Chapter 7. 一些常見的 Rings

(1) 假設 R 是一個 integral domain 且 $a, b \in R$.
 (a) 試證明 $\big(a\big) \subseteq \big(b\big)$ 若且唯若 $b \mid a$.
 (b) 試證明 $a \mid b$ 且 $b \mid a$ 若且唯若存在 $u \in R$ 是 unit 滿足 $a = ub$.
 (c) 試證明 R 中的 prime element 一定是 irreducible element.
 (d) 假設 $a, b \in R$ 是 prime 試證明 $a \mid b$ 若且唯若 $b \mid a$.

(2) 假設 R 是一個 integral domain 且 $f(x), g(x)$ 是 $R[x]$ 中非 0 的多項式.
 (a) 試證明 $\deg(f(x)+g(x)) \leq \max\{\deg(f), \deg(g)\}$ 且當 $\deg(f) \neq \deg(g)$ 時等號成立.
 (b) 試證明 $\deg(f(x)g(x)) = \deg(f(x)) + \deg(g(x))$.
 (c) 試說明若 R' 中有 zero divisor, 則在 $R'[x]$ 中必存在兩個非 0 的多項式 $f(x), g(x)$ 會使得 $\deg(f(x)g(x)) < \deg(f(x)) + \deg(g(x))$.

(3) 假設 F 試一個 field, $f(x), g(x) \in F[x]$. 我們稱 $f(x)$ 和 $g(x)$ 互質 *relatively prime* 如果 $\gcd(f(x), g(x))$ 是 $F[x]$ 中的 unit. 現假設 $f(x)$ 和 $g(x)$ 是 relatively prime.
 (a) 試證明若 $h(x) \in F[x]$ 滿足 $f(x) \mid g(x)h(x)$, 則 $f(x) \mid h(x)$.
 (b) 試證明若 $l(x) \in F[x]$ 滿足 $f(x) \mid l(x)$ 且 $g(x) \mid l(x)$, 則 $f(x)g(x) \mid l(x)$.

(4) 假設 F 是一個 field 且 $f(x) \in F[x]$ 其中 $\deg(f(x)) = 3$. 試證明 $f(x)$ 在 $F[x]$ 不是 irreducible 若且唯若存在 $r \in F$ 使得 $f(r) = 0$.

(5) 假設 F, K 皆為 field 且 $F \subseteq K$.
 (a) 若 $p(x) \in K[x]$ 且在 $K[x]$ 中是 prime, 試證明 $p(x)$ 在 $F[x]$ 中是 prime.
 (b) 試找到兩個 field F 和 K 滿足 $F \subseteq K$ 且在 $F[x]$ 中找到一個元素 在 $F[x]$ 是 prime 但在 $K[x]$ 不是 prime.
 (c) 假設 $f(x), g(x) \in F[x]$. 試證明 $f(x)$ 和 $g(x)$ 在 $K[x]$ 中是 relatively prime 若且唯若 $f(x)$ 和 $g(x)$ 在 $F[x]$ 是 relatively prime.

(6) 試證明 $\big(x^2+1\big)$ 是 $\mathbb{R}[x]$ 中的 maximal ideal 並證明 $\mathbb{R}[x]/\big(x^2+1\big) \simeq \mathbb{C}$.

(7) 令 $F = \mathbb{Z}/11\mathbb{Z}$, 已知 F 為一個 field.
 (a) 試證明 x^2+1 在 $F[x]$ 中是 irreducible 且 $F[x]/\big(x^2+1\big)$ 是一個有 11^2 個元素的 field.
 (b) 試證明 x^3+x+4 在 $F[x]$ 中是 irreducible 且 $F[x]/\big(x^3+x+4\big)$ 是一個有 11^3 個元素的 field.

(8) 假設 F 是一個 field.
 (a) 試證明 $F[x]$ 中存在無窮多個 monic irreducible polynomial.
 (b) 假設 F 是一個 finite field (即僅有有限個元素的 field). 試證明對任意 $n \in \mathbb{N}$ 皆存在 $p(x) \in F[x]$ 是 irreducible 且 $\deg(p(x)) > n$.

12 April, 2007

(9) 令 $f(x)=\frac{2}{3}x^3+\frac{5}{12}x^2+\frac{7}{18}x+\frac{1}{4}$, $g(x)=\frac{3}{4}x^4-\frac{5}{24}x^3-\frac{2}{9}x^2+\frac{7}{24}x+\frac{1}{27}$.
   (a) 試將 $f(x)$ 和 $g(x)$ 分別寫成 $f(x)=c(f)f^*(x)$ 以及 $g(x)=c(g)g^*(x)$ 之形式, 其中 $f^*(x)$ 和 $g^*(x)$ 是 primitive polynomials.
   (b) 試求 $f(x)+g(x)$ 以及 $f(x)g(x)$ 之content.

(10) 假設 $f(x),g(x)\in\mathbb{Q}[x]$.
   (a) 已知 $f(x),g(x)\in\mathbb{Z}[x]$. 試證明若 $f(x)g(x)$ 是 primitive polynomial 則 $f(x),g(x)$ 皆為 primitive polynomials.
   (b) 已知 $f(x)\in\mathbb{Z}[x]$ 是 primitive polynomial. 試證明若 $f(x)g(x)\in\mathbb{Z}[x]$ 則 $g(x)\in\mathbb{Z}[x]$.
   (c) 已知 $f(x)\in\mathbb{Z}[x]$ 是 primitive polynomial. 試證明 $f(x)$ 在 $\mathbb{Q}[x]$ 中是 prime 若且唯若 $f(x)$ 在 $\mathbb{Z}[x]$ 中是 prime.

(11) 假設 R 是一個 commutative ring 且 I 是 R 的一個 ideal. 考慮 $R[x]$ 和 $I[x]$ 分別是係數在 R 和 I 的多項式所成之集合.
   (a) 考慮一般多項式的加法及乘法試證明 $I[x]$ 會是 $R[x]$ 的一個 ideal.
   (b) 令 $\overline{R}=R/I$ 考慮函數 $\Phi:R[x]\to\overline{R}[x]$ 定義為: 若

$$f=a_nx^n+\cdots+a_1x+a_0 \text{ 則 } \Phi(f)=\overline{a_n}x^n+\cdots+\overline{a_1}x+\overline{a_0}.$$

   試證明 Φ 是一個 ring homomorphism.
   (c) 試證明 $R[x]/I[x]\simeq(R/I)[x]$ as a ring.
   (d) 試利用 (b) 中 Φ 是 homomorphism 的性質證明 Gauss Lemma: 即若 $f,g\in\mathbb{Z}[x]$ 是 primitive polynomial, 則 fg 也是 primitive polynomial.
   (e) 試利用 (b) 中 Φ 是 homomorphism 的性質證明 Eisenstein Criterion: 即若 $f(x)=x^n+a_{n-1}x^{n-1}+\cdots a_1x+a_0\in\mathbb{Z}[x]$ 且存在一質數 p 滿足 $p\mid a_{n-1},\ldots,p\mid a_1,p\mid a_0$ 但 $p^2\nmid a_0$, 則 $f(x)$ 在 $\mathbb{Z}[x]$ 中是 irreducible.

(12) 假設 F 是一個 field 且 $\phi:F[x]\to F[x]$ 是一個 ring homomorphism 滿足對任意 $a\in F$ 皆有 $\phi(a)=a$.
   (a) 試證明 ϕ 是 epimorphism 若且唯若 $\deg(\phi(x))=1$.
   (b) 試證明 ϕ 是 epimorphism 若且唯若 ϕ 是 isomorphism.
   (c) 試證明 ϕ 是 isomorphism 若且唯若存在 $a,b\in F$ 且 $a\neq 0$ 使得對任意 $f(x)\in F[x]$ 皆有 $\phi(f(x))=f(ax+b)$.
   (d) 假設 ϕ 是 isomorphism. 試證明 $f(x)\in F[x]$ 是 irreducible 若且唯若 $\phi(f(x))$ 是 irreducible.
   (e) 試證明若 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots a_1x+a_0\in\mathbb{Z}[x]$ 且存在一質數 p 滿足 $p\mid a_{n-1},\ldots,p\mid a_1,p\mid a_0$ 但 $p\nmid a_n$ 且 $p^2\nmid a_0$, 則 $f(x)$ 在 $\mathbb{Q}[x]$ 中是 irreducible.
   (f) 若 $p\in\mathbb{Z}$ 是一質數, 試證明 $f(x)=x^{p-1}+x^{p-2}+\cdots+x+1$ 在 $\mathbb{Q}[x]$ 中是 irreducible.

---

19 April, 2007

(13) 令 $Q(\mathbb{Z})$ 表示 $\mathbb{Z}$ 的 quotient field. 試找到一個 $Q(\mathbb{Z})$ 到 $\mathbb{Q}$ 的 ring isomorphism.

(14) 假設 R 是一個 field, $Q(R)$ 為其 quotient field. 試找到一個 R to $Q(R)$ 的 ring isomorphism.

(15) 假設 R 和 R' 為 integral domain 且 $Q(R), Q(R')$ 分別為 R 和 R' 的 quotient field.

  (a) 試證明若 $R \simeq R'$ as a ring, 則 $Q(R) \simeq Q(R')$ as a ring.

  (b) 試找到一個 $Q(R) \simeq Q(R')$ 但是 $R \not\simeq R'$ 的例子.

(16) 假設 R 是一個 commutative ring without zero divisor (有可能沒有 1).

  (a) 試證明可利用 integral domain 得到 quotient field 的方法得到 $Q(R)$ 且 $Q(R)$ 是一個 field.

  (b) 試證明存在一個 R 到 $Q(R)$ 的 ring monomorphism.

  (c) 試證明若 F 是一個 field 且存在一個從 R 到 F 的 ring monomorphism, 則存在一個 $Q(R)$ 到 F 的 ring monomorphism.

  (d) 試找到一個從 $Q(2\mathbb{Z})$ 到 $\mathbb{Q}$ 的 ring isomorphism.

Chapter 8. Integral domain 上的分解性質

(1) 假設 $d \in \mathbb{Q}[x]$ 是 $4x$ 以及 $2x^2$ 在 $\mathbb{Q}[x]$ 中的 greatest common divisor.
   (a) 試寫下 d 所有可能之形式
   (b) 試證明在 $\mathbb{Q}[x]$ 中 $(4x) + (2x^2) = (d)$.

(2) 假設 $d \in \mathbb{Z}[x]$ 是 $4x$ 以及 $2x^2$ 在 $\mathbb{Z}[x]$ 中的 greatest common divisor.
   (a) 試寫下 d 所有可能之形式
   (b) 試證明 在 $\mathbb{Z}[x]$ 中 $(4x) + (2x^2) \neq (d)$.

(3) 假設 R 是一個 integral domain, $a, b \in R$ 且 d 是 a, b 之一個 greatest common divisor.
   (a) 試證明 $d' \in R$ 是 a, b 之 一個 greatest common divisor 若且唯若存在 $u \in R$ 是 R 中之 unit 使得 $d' = ud$.
   (b) 假設 $a = da'$ 且 $b = db'$, 其中 $a', b' \in R$. 試證明 1 是 a' 和 b' 之一個 greatest common divisor.

(4) 假設 F 是一個 field. 試找到一函數 $\Phi : F \setminus \{0\} \to \mathbb{N} \cup \{0\}$ 使其符合 Euclidean domain 之要求,

(5) 假設 R 是一個 Euclidean domain 其中函數 $\Phi : R \setminus \{0\} \to \mathbb{N} \cup \{0\}$ 可使其符合 Euclidean domain 之要求.
   (a) 試證明若 $\alpha \in R$ 且對任意 $\beta \in R \setminus \{0\}$ 皆有 $\Phi(\alpha) \leq \Phi(\beta)$, 則 α 是 R 中的一個 unit.
   (b) 試找到一個 Euclidean domain R 及函數 Φ 以及 R 中的一個 unit α 使其不滿足對任意 $\beta \in R \setminus \{0\}$ 皆有 $\Phi(\alpha) \leq \Phi(\beta)$.

(6) 已知在 principle ideal domain 中一個 nontrivial ideal 是 maximal ideal 若且唯若是 prime ideal. 以下可看出若不是 principle ideal domain 這不一定對.
   (a) 試證明在 $\mathbb{Q}[x]$ 中 (x) 是 maximal ideal.
   (b) 試證明 x 在 $\mathbb{Z}[x]$ 中是一個 irreducible element.
   (c) 試證明在 $\mathbb{Z}[x]$ 中 (x) 是 prime ideal 但不是 maximal ideal.

(7) 假設 R 是一個 integral domain, 且 $a, b \in R$.
   (a) 若 $d \in R$ 滿足 $(a) + (b) = (d)$, 試證明 d 是 a, b 的 greatest common divisor.
   (b) 假設 R 是一個 principle ideal domain. 若 $d \in R$ 是 a, b 的 greatest common divisor, 試證明 $(a) + (b) = (d)$.
   (c) 試找到一例子說明 (b) 中確實需要 R 是 principle ideal domain 之假設才會對.

---

10 May, 2007

(8) 假設 R 是一個 integral domain 且 $a_1, \ldots, a_n \in R$. 我們定義 R 中滿足以下條件之 l 為 $a_1, \ldots, a_n$ 之 least common multiple:

甲: 對於所有 $i \in \{1, \ldots, n\}$ 皆有 $a_i | l$.

乙: 若 $m \in R$ 滿足對於所有 $i \in \{1, \ldots, n\}$ 皆有 $a_i | m$, 則 $l | m$.

(a) 試證明 $l \in R$ 滿足 $(a) \cap (b) = (l)$, 若且唯若 l 是 a, b 之一個 least common multiple.

(b) 假設 R 中任兩個元素的 least common multiple 皆存在, 試證明任取 $a_1, \ldots, a_n \in R$ 其 least common multiple 亦存在.

(c) 假設 R 是一個 unique factorization domain 且 $a, b \in R$. 試證明 a, b 的 least common multiple 必存在.

(d) 假設 R 是一個 unique factorization domain 且 d 為 a, b 之一個 greatest common divisor. 令 $a = da', b = db'$ 其中 $a', b' \in R$. 試證明 $a'b'd$ 為 a, b 之一個 least common multiple.

(e) 假設 R 是一個 unique factorization domain 且 $a, b \in R$. 試證明 $(a) \cap (b) = (ab)$ 若且唯若 a 和 b 的 greatest common divisor 是 unit.

(9) 假設 R 是一個 integral domain 且 $a_1, \ldots, a_n \in R$.

(a) 假設 d 是 $a_1, \ldots, a_n$ 的一個 greatest common divisor 且對任意 $i \in \{1, \ldots, n\}$, $a_i = a'_i d$, 其中 $a'_i \in R$. 試證明 $a'_1, \ldots, a'_n$ 的 greatest common divisor 必存在且是 R 中的 unit.

(b) 假設 R 是一個 unique factorization domain 且對任意 $i \neq j$, a_i 和 a_j 的 greatest common divisor 是一個 unit. 試證明 $a_1 \cdots a_n$ 是 $a_1, \ldots, a_n$ 的一個 least common multiple.

(10) 假設 R 是一個 integral domain 且符合以下兩個性質.

甲: 對任意 R 中無窮遞增的 principle ideal

$$(a_1) \subseteq (a_2) \subseteq \cdots \subseteq (a_n) \subseteq \cdots$$

皆存在 $m \in \mathbb{N}$, 使得對所有 $i \geq m$ 皆有 $(a_i) = (a_m)$.

乙: R 中的 irreducible element 皆為 prime element.

試證明 R 是一個 unique factorization domain.

(11) 假設 R 是一個 unique factorization domain 且不是一個 field. 令 $F = Q(R)$ 為 R 的 quotient field.

(a) 試證明若 $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots a_1 x + a_0 \in R[x]$ 且存在一個 R 中的 irreducible element p 使得在 R 中 $p \mid a_{n-1}, \ldots, p \mid a_1, p \mid a_0$ 但 $p \nmid a_n$ 且 $p^2 \nmid a_0$, 則 $f(x)$ 在 $F[x]$ 中是 irreducible.

(b) 試證明對任意 $n \in \mathbb{N}$ 皆存在 $p(x) \in R[x]$ 是 irreducible 且 $\deg(p(x)) = n$.

Chapter 9. 初級 Field 的性質

(1) 假設 R, R' 皆為 ring with 1 且 $\phi : R \to R'$ 是一個 nontrivial 的 ring homomorphism.

  (a) 若已知 R' 沒有 zero divisor, 試證明 $\phi(1_R) = 1_{R'}$ ($1_R, 1_{R'}$ 分別表 R 和 R' 乘法的 identity).

  (b) 若已知 R 是一個 field 試證明 $\phi(R)$ (即 ϕ 的 image) 也是一個 field.

(2) 假設 R' 是一個 integral domain 且 R 是 R' 的 subring 並假設 1_R 為 R 乘法的 identity. 若 $1_{R'}$ 為 R' 之乘法 identity, 試證明 R 亦為一個 integral domain 且 $1_R = 1_{R'}$.

(3) 假設 F, K 皆為 field, 若 F 中存在一個 subfield 和 K 是 isomorphic, 為了方便記我們直接說 K 是 F 的 subfield.

  (a) 試證明 $\mathbb{Q}$ 會是 F 的 subfield 或是存在一質數 p 使得 $\mathbb{Z}/p\mathbb{Z}$ 是 F 的 subfield.

  (b) 試證明不可能同時 $\mathbb{Q}$ 和 $\mathbb{Z}_p$ 皆為 F 的 subfield.

  (c) 當 p 是質數時, 試證明所有有 p 個元素的 field 皆和 $\mathbb{Z}/p\mathbb{Z}$ isomorphic (今後為了方便記, 我們以 $\mathbb{F}_p$ 表示有 p 個元素的 field.)

(4) 假設 F 是一個 field 且 $\phi : F \to F$ 是一個 nontrivial 的 ring homomorphism.

  (a) 試證明若 $\mathbb{Q}$ 是 F 的一個 subfield, 則 ϕ 一定是 $\mathbb{Q}$-linear, 即對任意 $a, b \in F$ 及 $r \in \mathbb{Q}$ 皆有 $\phi(ra + b) = r\phi(a) + \phi(b)$.

  (b) 試證明若 $\mathbb{F}_p$ 是 F 的 subfield, 則 ϕ 一定是 $\mathbb{F}_p$-linear.

  (c) 試證明若 F 是一個 finite field, 則 ϕ 一定是一個 isomorphism.

(5) 假設 F 是一個 field of characteristic p. 對任意 $n \in \mathbb{N}$ 考慮 $\uparrow_{p^n} : F \to F$ 定義為 $\uparrow_{p^n}(\alpha) = \alpha^{p^n}, \forall \alpha \in F$.

  (a) 試證明 $\uparrow_{p^n}$ 是一個 ring homomorphism.

  (b) 假設 F 是一個 finite field, 給定 $n \in \mathbb{N}$ 試證明對任意 $a \in F$ 皆存在唯一的 $b \in F$ 使得 $b^{p^n} = a$.

  (c) 假設 F 是一個有 p^n 個元素的 finite field (以後我們會知道所有的 finite field 的個數皆為這種形式). 試證明 $\uparrow_{p^n}$ 是一個 identity map, 也就是說對任意 $a \in F$ 皆有 $\uparrow_{p^n}(a) = a$.

(6) 以下是探討 $\mathbb{Q}[x]/\big(x^2-1\big)$ 以及 $\mathbb{Q}[x]/\big(x^2+1\big)$ 看成 vector space over $\mathbb{Q}$ 以及看成 ring 的差異.

(a) 將 $\mathbb{Q}[x]/\big(x^2-1\big)$ 以及 $\mathbb{Q}[x]/\big(x^2+1\big)$ 看成 vector space over $\mathbb{Q}$. 試證明 $\mathbb{Q}[x]/\big(x^2-1\big)$ 和 $\mathbb{Q}[x]/\big(x^2+1\big)$ 是一個 isomorphic vector space over k.(也就是說它們之間存在一個一對一且映成的 $\mathbb{Q}$-linear transformation).

(b) 將 $\mathbb{Q}[x]/\big(x^2-1\big)$ 以及 $\mathbb{Q}[x]/\big(x^2+1\big)$ 看成式 ring, 試證明 $\mathbb{Q}[x]/\big(x^2-1\big)$ 以及 $\mathbb{Q}[x]/\big(x^2+1\big)$之間不可能找到一個 ring isomorphism.

(7) 令 $\mathbb{C}$ 和 $\mathbb{R}$ 分別表示複數及實數所成之 field.

(a) 試證明 $[\mathbb{C}:\mathbb{R}]=2$.

(b) 證明若 $\alpha\in\mathbb{C}$, 則必存在 $f(x)\in\mathbb{R}[x]$ 其中 $\deg(f(x))=2$ 使得 $f(\alpha)=2$.

(c) 已知所有實係數多項式皆有一個複數根. 依此證明所有 $\mathbb{R}[x]$ 中的 ireeducible polynomial 皆為一次或二次實係數多項式.

(8) 假設 L/F 是一個 field extension.

(a) 假設 $\alpha\in L$ 是 transcendental over F. 試證明若 $f(x)\in F[x]$, 其中 $\deg(f(x))\geq 1$, 則 $f(\alpha)$ 也是 transcendental over F.

(b) 假設 $\alpha\in L$, $f(x)\in F[x]$ 且 $\deg(f(x))\geq 1$. 若已知 $f(\alpha)$ 是 algebraic over F, 試證明 α 亦為 algebraic over F.

(9) 假設 L/F 是一個 finite extension 且 V 是一個 finite dimensional vector space over L. 試證明 V 是一個 finite dimensional vector space over F 且 $\dim_F(V)=[L:F]\dim_L(V)$.

(10) 假設 L/F 是一個 field extension. 若 $\alpha\in L$, 我們令

$$F[\alpha]=\{f(\alpha)\mid f(x)\in F[x]\}.$$

(a) 試證明 $F[\alpha]$ 是一個 vector space over F.

(b) 試證明 $F[\alpha]$ 是一個 integral domain.

(c) 假設 $\alpha\in L$ 是 transcendental over F. 試證明 $F[\alpha]\simeq F[x]$ as a ring.

(d) 假設 $\alpha\in L$ 是 algebraic over F, 且存在 $f(x)\in F[x]$ 其 degree 為 n, 使得 $f(\alpha)=0$. 試證明 $F[\alpha]$ 是一個 finite dimensional vector space over F 且 $\dim_F(F[\alpha])\leq n$.

(e) 假設 $\alpha\in L$ 是 algebraic over F. 試證明存在 $F[x]$ 中的 irreducible polynomial $p(x)$ 使得 $F[\alpha]\simeq F[x]/\big(p(x)\big)$.

Chapter 10. 中級 Field 的性質

(1) 已知 π 是 transcendental over $\mathbb{Q}$. 試證明 $\mathbb{Q}[\sqrt{\pi}]$ 不是一個 field 但 $\mathbb{R}[\sqrt{\pi}]$ 是一個 field.

(2) 假設 L/F 是一個 field extension, $\alpha, \beta \in L$. 已知 α 是 algebraic over F 且 β 是 transcendental over F.

  (a) 假設 $f(x) \in F[x]$. 試證明 $f(\alpha)$ 是 algebraic over F 且其 over F 的 degree 小於等於 α over F 的 degree.

  (b) 若 $f(x), g(x) \in F[x]$ 且 $\deg(g(x)) \geq 1$. 試證明 $f(\alpha) + g(\beta)$ 是 transcendental over F.

(3) 假設 L/F 是一個 field extension 且 $\alpha \in L$ 是 algebraic over F of degree n. 試證明 $1, \alpha, \ldots, \alpha^{n-1}$ 是 $F(\alpha)$ over F 的一組 basis.

(4) 考慮 $\mathbb{Q}(\sqrt{2})$ 和 $\mathbb{Q}(\sqrt{3})$ 為 $\mathbb{Q}$ 的 extension.

  (a) 試證明 $\mathbb{Q}(\sqrt{2}+3) = \mathbb{Q}(\sqrt{2})$.

  (b) 試證明 $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}]$ 但 $\mathbb{Q}(\sqrt{2})$ 和 $\mathbb{Q}(\sqrt{3})$ 並不 isomorphic as rings.

  (c) 利用 (b) 得知 $\mathbb{Q}(\sqrt{2}) \neq \mathbb{Q}(\sqrt{3})$ 並依此證明 $[\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}] = 4$.

(5) 假設 p 是一個奇質數, 而 L/F 是一個 finite extension of degree p.

  (a) 試證明若 $\alpha \in L$ 但 $\alpha \notin F$, 則 $F(\alpha) = L$.

  (b) 試證明若 $F(\alpha) = L$ 則 $F(\alpha^2) = L$.

(6) 假設 L/F 是一個 field extension.

  (a) 假設 $\alpha, \beta \in L$ 為 algebraic over F 且其 over F 的 degree 分別為 m, n 其中 m, n 互質. 試證明 $[F(\alpha, \beta) : F] = mn$.

  (b) 假設 $\gamma \in L$ 是 algebraic over F 試證明存在 $n \in \mathbb{N}$ 使得對所有 $m > n$ 解滿足 $F(\gamma^{2^m}) = F(\gamma^{2^n})$

(7) 假設 L/K 是一個 algebraic extension 且 K/F 也是 algebraic extension. 試證明 L/F 也是 algebraic extension.

(8) 假設 L/F 是一個 field extension 且 L 和 F 分別為元素個數為 p^n 和 q^m 的 finite field, 其中 p, q 為質數.

(a) 試證明 $p = q$ 且 $m|n$.

(b) 試證明若 $p(x) \in F[x]$ 是一個 irreducible polynomial 且 $p(x)$ 在 L 中有一個根, 則 $p(x)$ 在 L 中可完全分解 (splits completely).

(c) 試證明若 $p(x) \in F[x]$ 是一個 irreducible polynomial 且 $p(x)$ 在 L 中有一個根, 則 $\deg(p(x))|\frac{n}{m}$.

(9) 假設 F 是一個 finite field 且 $p(x), q(x) \in F[x]$ 皆為 irreducible polynomial.

(a) 若 $\deg(p(x)) = \deg(q(x))$, 試證明 $F[x]/\big(p(x)\big) \simeq F[x]/\big(q(x)\big)$ as rings.

(b) 試證明 $\deg(p(x))|\deg(q(x))$ 若且唯若存在一個從 $F[x]/\big(p(x)\big)$ 映射到 $F[x]/\big(q(x)\big)$ 的 nontrivial ring homomorphism.

(10) 令 $\mathbb{F}_q$ 表示元素個數為 q 的 finite field.

(a) 試證明若 $2 \mid q$, 則對任意 $a \in \mathbb{F}_q$, $x^2 - a$ 在 $\mathbb{F}_q[x]$ 中一定不是 irreducible.

(b) 試證明若 $2 \nmid q$, 則必存在 $a \in \mathbb{F}_q$ 使得 $x^2 - a$ 在 $\mathbb{F}_q[x]$ 中是 irreducible.

(c) 試創出一個 finite field F 使得 $F \simeq \mathbb{F}_4$, 並找出 F^* 的 generater.

(d) 試創出一個 finite field F 使得 $F \simeq \mathbb{F}_9$, 並找出 F^* 的 generater.

(11) 令 F 是一個 field, 定義一個函數 $\delta : F[x] \to F[x]$ 其中若

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in F[x],$$

則定義

$$\delta(f(x)) = n a_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1.$$

假設 $f(x) \in F[x]$ 且存在一個 field extension L/F 使得 $f(x)$ 在 L 中有重根. 則我們便稱 $f(x)$ 有重根.

(a) 假設 $f(x), g(x) \in F[x]$, 試證明 $\delta(f(x) + g(x)) = \delta(f(x)) + \delta(g(x))$.

(b) 假設 $f(x), g(x) \in F[x]$, 試證明 $\delta(f(x)g(x)) = f(x)\delta(g(x)) + \delta(f(x))g(x)$.

(c) 假設 $f(x) \in F[x]$ 有重根. 試證明 $f(x)$ 和 $\delta(f(x))$ 在 $F[x]$ 中有 nontrivial 的公因式.

(d) 試證明若 $p(x) \in F[x]$ 是一個 irreducible polynomial 且有重根, 則 $\delta(p(x))$ 是零多項式.

(e) 試證明若 F 的 characteristic 為 0, 則 $F[x]$ 中所有的 irreducible polynomial 都不會有重根.

(f) 試證明若 F 是一個 finite field, 則 $F[x]$ 中所有的 irreducible polynomial 都不會有重根.

(12) 假設 F 是一個 field, 令 F^* 表示 F 中非 0 元素所成之乘法群.

(a) 若 G 是 F^* 的一個 finite subgroup, 試證明 G 是一個 cyclic group.

(b) 試證明在 $\mathbb{C}^*$ 中, 給定 $n \in \mathbb{N}$ 皆存在唯一的一個 order 為 n 的 subgroup.

——— 全劇終 ———

14 June, 2007