二次虛數體 R($\sqrt{-21}$) 中之一例

AN EXAMPLE IN IMAGINARY QUADRATIC FIELD R($\sqrt{-12}$)

徐 道 寧

BY HSÜ TAO-NING

作者於 Über den Hauptidealsatz für imaginäre quadratische Zahlkörper 一文 (Journal für die reine und angewandte Mathematik, 1963) 中曾就二次虛數體 R($\sqrt{m}$) 中提出並證明下之定理，其中 R 表有理數體，m 爲一無平方因子之負整數：

定理 4 (第 II 章，§2) 除 $m=-1$ 或 $m=-3$ 二特款外，當 $m\equiv 0 \bmod. 3$ 而 $\not\equiv 3 \bmod. 4$ 或 $m \not\equiv 0 \bmod. 3$ 而 $\equiv 3 \bmod. 4$ 時 R($\sqrt{m}$) 之理想數類中恰有一半不含有 $N(\mathfrak{a})\equiv 1 \bmod. 12$ 之理想數 $\mathfrak{a}$。若 $m\equiv 0 \bmod. 3$ 且 $m\equiv 3 \bmod. 4$，則僅有四分之一類中含有 $N(\mathfrak{a})\equiv 1 \bmod. 12$ 之 $\mathfrak{a}$。

因 $m=-1$ 或 $=-3$ 時絕對類數等於 1，故此定理不僅證明 H. Hasse 於 Zum Hauptidealsatz der komplexen Multiplikation 一文 (載於 Monatshefte für Mathematik und Physik 38(1931), 315—322 頁) 中及該文中所提及之 W. Schäfer 之博士論文 Beweis des Hauptidealsatzes der Klassenkörpertheorie für den Fall der komplexen Multiplikation (Halle 1929) 中所稱每一類中必有此等理想數或一級質理想數一事之錯誤，且明確指出，何時全部可有 (定理 3 中證明除合定理 4 條件之 m 外 R($\sqrt{m}$) 中各類均有)，何時僅其半而何時則僅四分之一。該文中此一定理本作預備之用，未曾列有實例，今作一例以爲補充。

二次虛數體 R($\sqrt{-21}$) 中 $m=-21$，合於該定理下半之條件，依定理僅四分之一類中有合於 $N(\mathfrak{a})\equiv 1 \bmod. 12$ 之 $\mathfrak{a}$，此一數體之理想數共分四類 A, B, C, D, 可分別以 $\mathfrak{a}=(1)$, $\mathfrak{b}=(5, 3+\sqrt{-21})$, $\mathfrak{c}=(3, \sqrt{-21})$ 及 $\mathfrak{d}=(2, 1+\sqrt{-21})$ 作爲代表 (J. Sommer: Vorlesung über Zahlentheorie: Einführung in die Theorie der algebraischen Zahlkörper, 附表），體 R（$\sqrt{-21}$）中之整數均作 $\alpha+b\sqrt{-21}$ 之形，其中 α, b 為有理整數，其模 $N(\alpha+b\sqrt{-21})=\alpha^2+21b^2$, α^2, b^2 或 $\equiv 1 \mod 4$, 或 $\equiv 0 \mod 4$，而 $21 \equiv 1 \mod 4$, $\equiv 0$ med. 3，配合之可得 $N=N(\alpha+b\sqrt{-21})$ 對 12 之各種可能情形：

1. $\alpha^2\equiv 0 \mod 4$, $b^2\equiv 0 \mod 4$. 此時 $21b^2\equiv 0 \mod 4$ 因而 $N\equiv 0 \mod 4$, $N\equiv 0, 4, 8 \mod 12$.

2. $\alpha^2\equiv 1 \mod 4$, $b^2\equiv 1 \mod 4$. 此時 $N\equiv 2 \mod 4$, 而 $N\equiv 2, 6, 10 \mod 12$.

3. $\alpha^2\equiv 1 \mod 4$, $b^2\equiv 0 \mod 4$, 此時 $21b^2\equiv 0 \mod 12$. 令 $\alpha\equiv 2m+1$, 則 $\alpha^2=4m(m+1)+1$. $m\equiv 0 \mod 3$ 時 $\alpha^2\equiv 1 \mod 12$, 故 $N\equiv 1 \mod 12$; $m\equiv 1 \mod 3$ 時 $\alpha=2m+1\equiv 0 \mod 3$, $\alpha^2\equiv 0 \mod 3$, 故 $N\equiv 9 \mod 12$; $m\equiv 2 \mod 3$ 時 $m+1\equiv 0 \mod 3$, 故 $\alpha^2=4m(m+1)+1\equiv 1 \mod 12$ 而 $N\equiv 1 \mod 12$. 綜上所得 $N\equiv 1$ 或 $9 \mod 12$.

4. $\alpha^2\equiv 0 \mod 4$, $b^2\equiv 1 \mod 4$. 此時 $21b^2\equiv 9 \mod 12$. 令 $\alpha=2^h m$, $m=2n+1$, 則 $\alpha^2=2^{2h}(2n+1)^2$. 由 3. 知 $(2n+1)^2$ 或 $\equiv 1 \mod 12$, 或 $\equiv 0 \mod 3$ 後者使 $\alpha^2\equiv 0 \mod 12$, 前者使 $\alpha^2\equiv 2^{2h} \mod 12$, 因 $\alpha^2\equiv 0 \mod 4$ 而 $h\neq 0$, 故 $\alpha^2\equiv 4 \mod 12$. $N\equiv 9 \mod 12$ 或 $\equiv 1 \mod 12$.

由上之結果知體 R（$\sqrt{-21}$）中任一整數 $\alpha+b\sqrt{-21}$ 之模 N 或 $\equiv 1 \mod 12$ 或 $\equiv 9 \mod 12$, 或與 2 及其各整倍數對 12 同餘，理想數類 A 全由主理想數集成，$N(\alpha+b\sqrt{-21})\equiv 1 \mod 12$ 時令 $\overline{\mathfrak{m}}=(\alpha+b\sqrt{-21})$ 則 $N(\overline{\mathfrak{m}})\equiv 1 \mod 12$. 故此類中有模為 $\equiv 1 \mod 12$ 之理想數, $N(\mathfrak{b})=5$, $N(\mathfrak{c})=3$, $N(\mathfrak{d})=2$, 乘以模 $\equiv 1, 9$; 或 2, 4, 6, 8, 10 之整數均不能得 $\equiv 1 \mod 12$ 之數，故知 B, C, D, 三類中一切理想數之模均不合 $\equiv 1 \mod 12$ 之條件.