取 $\eta=\frac{1}{2}(m+n\sqrt{-11})\in R$. 则.

$$\left|\frac{\alpha}{\beta}-\eta\right|^2=\left|(r-\frac{m}{2})+(s-\frac{n}{2})\sqrt{-11}\right|^2=\frac{(2r-m)^2}{4}+\frac{11}{4}(2s-\frac{n}{2})^2$$

$$\leq\frac{1}{4}+\frac{11}{4}\times\frac{1}{4}=\frac{15}{16}<1$$

$\Rightarrow$ 令 $\gamma=\alpha-\beta\eta$. 有 $|\alpha-\beta\eta|^2 \Leftrightarrow \beta=|\gamma|^2<|\beta|^2$.

$\therefore$ R 按映射 $N(w)=|w|^2$ 构成 Euclid 整环。

---

14. 设F为 $q=p^n$ 元域，p为素数。对 $\alpha\in F$ 让 $\sigma(\alpha)=\alpha^p$，试证 σ 属于域F的自同构群 Aut(F).

证明：

环同态 $\begin{cases}\sigma(\alpha\beta)=(\alpha\beta)^p=\alpha^p\beta^p=\sigma(\alpha)\sigma(\beta)\\ \sigma(\alpha+\beta)=(\alpha+\beta)^p=\alpha^p+\beta^p=\sigma(\alpha)+\sigma(\beta)\end{cases}$

$\therefore$ σ 为F的自同态.

若 $\sigma(\alpha)=\sigma(\beta)$ 即 $\alpha^p=\beta^p$.

$\because$ $(\alpha-\beta)^p+\beta^p=\alpha^p$ $\Rightarrow$ $\therefore$ $(\alpha-\beta)^p=0$

$\Rightarrow$ $\alpha=\beta$. 故 σ 为单射 ($\alpha^p\neq\beta^p$ 时 $\alpha\neq\beta$ 故单射. 在 $(\alpha-\beta)^p+\beta^p=((\alpha-\beta)+\beta)^p=\alpha^p$ 故 $(\alpha-\beta)^p\neq0$ 故 $\alpha\neq\beta$.)

又 $|F|<\infty$ 故 σ 为置换(双射)

故 $\sigma\in$ Aut(F)

$\forall\alpha\in F$ $\sigma(\alpha^{p^{n}})=\alpha^{p^n}=\alpha$.

15. 设F为 p^n 元有限域，p为素数。对 $\alpha\in F$，让 $\sigma(\alpha)=\alpha^p$. 并让E表示F的最小子域 $\{me: m\in\mathbb{Z}\}$，证明 σ 属于 Galois 群 $Gal(F/E)=\{\tau\in Aut(F): \forall a\in E\ (\tau(a)=a)\}$，且 σ 的阶 $o(\sigma)$ 等于 $n=[F:E]$.

证明：

$\forall a\in E$. 是 $\sigma(a)=a^p=\underline{a^{|E|}=a}$ (对域E) $\therefore$ $\sigma\in Gal(F/E)$.

又由于 $|F|=p^n$，$\alpha\in F$ 时 $\underline{\alpha^{p^n}=\alpha}$ (对域F) 即 $\sigma^n(\alpha)=\alpha$ 故 $\sigma^n=I$ (恒等变换)

假如有 $0<k<n$ 使 $\sigma^k=I$. 则 $\forall\alpha\in F$，有 $\alpha^{p^k}=\alpha$. 于是

$x^{p^k}-x=0$ 在F中有 $|F|=p^n>p^k$ 个根 (所有元均符合). 这不可能！

因此 σ 的阶正好是 $n=[F:E]$

$\sigma^n=I$

$\sigma^k(a)=a$

$a^k=a$

而 $a=\alpha^p$

$\alpha^{p^k}=\alpha^p=\alpha$ (域E)