八、（每小题5分，共10分）设 I 为交换幺环 R 的理想，且 $I\subseteq\bigcup_{i=1}^{n}P_i$，其中 $P_1,\dots,P_n$ 为 R 的素理想。

(1) 证明 $n>1$ 时必有 $1\leqslant j\leqslant n$ 使得 $I\subseteq\bigcup_{i\neq j}P_i$. [提示: 不然可取 $a_j\in I\setminus\bigcup_{i\neq j}P_i$ $(j=1,\dots,n)$, 然后考察元素 $a=a_1\cdots a_{n-1}+a_n$.]

假如不然，则对 $j=1,\dots,n$ 有 $a_j\in I$ 使 $a_j\notin\bigcup_{i\neq j}P_i$. 令 $a=a_1\cdots a_{n-1}+a_n$.
注意 $a_j\in P_j$ 但 $i\neq j$ 时 $a_j\notin P_i$. 因此 $a_1\cdots a_{n-1}\in P_1,\dots,P_{n-1}$ 但不属于 P_n.
a_n 属于 P_n 但不属于 $P_1,\dots,P_{n-1}$. 故 $a=a_1\cdots a_{n-1}+a_n$ 不属于 $P_1,\dots,P_{n-1},P_n$
这与 $a\in I$ 相矛盾.

(2) 利用（1）证明有 $1\leqslant i\leqslant n$ 使得 $I\subseteq P_i$.

对 n 归纳. $n=1$ 时显然.
设 $n>1$ 且对 $n-1$ 有所需结论. 依(1)有 j 使 $I\subseteq\bigcup_{i\neq j}P_i$.
根据归纳假设必有 $i\neq j$ 使 $I\subseteq P_i$.

九、（每小题5分，共10分）设 F 为 $q=p^n$ 元有限域，其中 p 为素数。

(1) 证明域 F 的特征为 p.

因 $|F|<\infty$, F 的特征不是 0, 从而是个素数 p'.
F 是 $E=\{me: m\in\mathbb{Z}\}$ (F 的素子域) 的有限扩张, 从而 $|F|$ 为 $|E|=p'$ 的幂次.
而 $|F|=p^n$, 故 $p'=p$.

(2) 对 $\alpha\in F$ 让 $\sigma(\alpha)=\alpha^p$, 试证 σ 属于域 F 的自同构群 $\mathrm{Aut}(F)$.

$\ker\sigma=\{\alpha\in F: \sigma(\alpha)=0\}=0$, $F/\ker\sigma\cong\mathrm{Im}\,\sigma$, $|\mathrm{Im}\,\sigma|=|F/0|=|F|$

$\sigma(\alpha\beta)=(\alpha\beta)^p=\alpha^p\beta^p=\sigma(\alpha)\sigma(\beta)$, $\sigma(\alpha+\beta)=(\alpha+\beta)^p=\alpha^p+\beta^p=\sigma(\alpha)+\sigma(\beta)$,
故 σ 是 F 的自同态. 如果 $\sigma(\alpha)=\sigma(\beta)$, 即 $\alpha^p=\beta^p$, 则
因 $(\alpha-\beta)^p+\beta^p=\alpha^p$ 而有 $(\alpha-\beta)^p=0$ 从而 $\alpha=\beta$. 故 σ 是单射.
又 $|F|<\infty$ 故 σ 是 F 的置换. 因此 $\sigma\in\mathrm{Aut}(F)$.

十、（10分）以下两小题选做一题

(a) 沿用第九题记号，并让 E 表示 F 的最小子域 $\{me: m\in\mathbb{Z}\}$（其中 e 为域的乘法单位元），证明 σ 属于 Galois 群 $\mathrm{Gal}(F/E)=\{\tau\in\mathrm{Aut}(F): \forall a\in E(\tau(a)=a)\}$，且 σ 的阶 $o(\sigma)$ 等于 $n=[F:E]$.

指数

~~(b) 设 R 为幺环，且对任何 $x\in R$ 都有 $x^2=x$, 试证 R 为交换环.~~

(a) $E=\{me: m\in\mathbb{Z}\}$ 为 F 的素子域. 对 $a\in E$, $a^p=a^{|E|}=a$. 故 $\sigma\in\mathrm{Gal}(F/E)$
由于 $|F|=p^n$, $\alpha\in F$ 时 $\alpha^{p^n}=\alpha$, 即 $\sigma^n(\alpha)=\alpha$. 故 $\sigma^n=I$.
假如有 $0<k<n$ 使 $\sigma^k=I$, 则对任何 $\alpha\in F$ 有 $\alpha^{p^k}=\alpha$, 于是
$x^{p^k}-x=0$ 在 F 中有 $|F|=p^n>p^k$ 个根, 这不可能. 因此
σ 的阶恰好是 $n=[F:E]$.

~~(b) ... $x+y=(x+y)^2=(x+y)(x+y)=x^2+xy+yx+y^2=x+y+xy+yx$ ... $=yx$ ... R 为交换环。~~