Mid.

问题一：(1) $S \subseteq G$, $S \neq \phi$.

$e = 1$

$\forall a, b \in S$. $\exists m, n \in G$, $a = m^2$, $b = n^2$

则 $ab^{-1} = m^2 n^{-2} = (mn^{-1})^2 \in S$

$\therefore S$ 是 G 的子群

(2) $|G| = p-1$

$\forall s \in S$. $\exists g. g \in G$, $s = g^2 = (-g)^2$

$s^{\frac{p-1}{2}} = g^{p-1} = e$ $\therefore \frac{p-1}{2} \geq |S|$.

$\because |G| = p-1$ $\therefore \exists g$. $|g| = p-1$

取 $s = g^2$, 则 $|s| = \frac{p-1}{2}$.

$\therefore \exists s$, $|s| = \frac{p-1}{2}$

$\therefore |S| \leq \frac{p-1}{2}$

$\therefore |S| = \frac{p-1}{2}$

$\therefore [G:S] = |G| / |S| = 2$

(3) 假设$\exists a\in G$, 使$a,-a\notin S$

$\because -1\notin S$, $|G|=p-1$, $S\leq G$.

$\therefore$ ~~$\#$~~ $|S|\leq p-2$ $\because [G:S]\geq 2$.

$\therefore \exists b\in G$, 使$b,-b\in S$

$\therefore b(-b)^{-1}=-1\in S$, 矛盾

$\therefore \forall a\in G$, 有$a\in S$或$-a\in S$

~~设R'关于+为~~ ~~R-R~~

~~R'=R∪{e}~~

~~$\forall a\in R$, $ae=ea=a$~~

问题二: $\forall a\in R$, $ae=ea=a$

$\because e\in R'$ $\therefore ne\in R'$, $\forall n\in\mathbb{Z}$

$\forall a\in R$, $a+ne=ne+a\in R'$

可使~~$\forall r\in R'$~~, ~~$r=a+ne$~~ $\exists a\in R$, $n\in\mathbb{Z}$, $r=a+ne$.

R的"+"在R'中为代数运算

~~$\forall a_1,a_2\in R'$, $a_1+a_2=$~~

$\forall r_1,r_2,r_3\in R'$, $r_1=a_1+n_1e$, $r_2=a_2+n_2e$, $r_3=a_3+n_3e$,

$(r_1+r_2)+r_3=a_1+a_2+a_3+(n_1+n_2+n_3)e=r_1+(r_2+r_3)$

$0+r_1=r_1+0=r_1$, $-r_1=-a_1-n_1e$.

$r_1+r_2=a_1+a_2+(n_1+n_2)e=r_2+r_1$

$\therefore R'$在"+"上为阿贝尔群

$(r_1\cdot r_2)\cdot r_3=a_1a_2a_3+a_1n_2en_3e+n_1ea_2n_3e+n_1en_2ea_3+n_1ea_2a_3$

$+a_1n_2ea_3+a_1a_2n_3e+n_1en_2en_3e=r_1(r_2\cdot r_3)$

NO.

Date

$r_1\cdot(r_2+r_3)=$ ~~a_1a_2~~ $a_1a_2+a_1a_3+n_1en_2e+n_1en_3e+a_1n_2e+a_1n_3e$

$+n_1ea_2+n_1ea_3=$ $r_1\cdot r_2+r_1\cdot r_3$

同理 $(r_2+r_3)\cdot r_1=$ $r_2\cdot r_1+r_3\cdot r_1$

$\therefore R'$ 在 "$\cdot$" 上满足结合律,

且 R' 满足分配律

$\therefore (R',+,\cdot)$ 为环, 其中 $\cdot$ 就是 R 的 $\cdot$.

且 $R\subseteq R'$, $R\subseteq R'$

$\therefore R$ 为 R' 的子环