Problem 73

Let $R \coloneqq \mathbb{Z}[\sqrt{p}]$. Given any element $\alpha \in R$, denote by $\overline{\alpha}$ the conjugate of α, i.e. the image of α under the field automorphism $\sqrt{p} \mapsto -\sqrt{p}$ of $\mathbb{Q}(\sqrt{p})$. Note that $\alpha \mapsto \overline{\alpha}$ is a ring automorphism of R, and therefore $\alpha \,|\, \beta$ in R iff $\overline{\alpha} \,|\, \overline{\beta}$ in R.

Suppose R is a UFD. We show that this implies that 2 has no irreducible factors. Since this contradicts the fact that in a Nötherian domain, such as R, every non-unit can be factored into irreducibles, R must not be a UFD.

Suppose $\gamma \in R$ is an irreducible factor of 2. Then $\overline{\gamma} \,|\, \overline{2} = 2$, so since R is a UFD, $N(\gamma) = \gamma\overline{\gamma} \,|\, 2$ in R and hence in $\mathbb{Z}$ (if $2 = (r + s\sqrt{p})N(\gamma)$, then $s = 0$ since $N(\gamma) \in \mathbb{Z}$, so $2 = rN(\gamma)$). But γ is irreducible and therefore a non-unit, so $|N(\gamma)| \neq 1$. Thus, $|N(\gamma)| = 2$.

Next, write γ as $r + s\sqrt{p}$, where $r, s \in \mathbb{Z}$. Since $|r^2 - s^2p| = |N(\gamma)| = 2$, we have in particular that

$$r^2 - s^2p \equiv 2 \pmod 4.$$

Using the fact that p, being the sum of two squares, is congruent to 1 modulo 4, this becomes

$$r^2 - s^2 \equiv 2 \pmod 4.$$

But this is impossible, since the only possible values of $r^2 - s^2 \bmod 4$ are $0 = 1 - 1 = 0 - 0$ and $1 = 1 - 0 = 0 - 1$. Thus, 2 has no irreducible factors.