M2P4 Rings and Fields
Answers Sheet 5.

1. If $p = x^2+2y^2$ then $p \nmid y$ so $yz \equiv 1 \bmod p$ for some z; hence $(xz)^2 \equiv -2 \bmod p$ and $p \equiv 1$ or $3 \bmod 8$.

Assume that $p \equiv 1$ or $3 \bmod 8$. Work in the PID $\mathbb{Z}[\sqrt{-2}]$. For some integer x we have $p \mid (x^2+2) = (x+\sqrt{-2})(x-\sqrt{-2})$. But $p \nmid (x+\sqrt{-2})$ and $p \nmid (x-\sqrt{-2})$. Therefore, p is not irreducible. Say $p = (a+b\sqrt{-2})(c+d\sqrt{-2})$. Then $p^2 = (a^2+2b^2)(c^2+2d^2)$, so $p = a^2+2b^2$.

2. (1) x^2+1 is irreducible in $\mathbb{Z}_3[x]$. Therefore, I is a maximal ideal and R/I is a field. The elements of R/I have the form $I+a+bx$ where $a, b \in \mathbb{Z}_3$, so R/I has 9 elements.

(2) The order of an element in F^* divides 8. Now, $(I+1+x)^2 = I+1+2x+x^2 = I+2x$ and $(I+1+x)^4 = I+x^2$. Hence $I+1+x$ has order 8, and F^* is cyclic.

3. (1) Let $\varphi(a+ib) = a^2+b^2$. Since $\varphi(3+2i) = 13$, we deduce that $3+2i$ is irreducible. Also, 3 is irreducible, since $\varphi(3) = 9$ and $\varphi(a+ib)$ is never 3. Therefore, $3R$ and $(3+2i)R$ are maximal ideals of the PID R.

(2) If $I = 3R$ then every element of R/I can be written uniquely in the form $I+a+ib$ with $0 \le a \le 2$ and $0 \le b \le 2$, so R/I has 9 elements.

If $I = (3+2i)R$ then $13 \in I$ since $13 = (3+2i)(3-2i)$. Moreover, $(8+i)-7(3+2i) = 13(-1-i) \in I$ so $8+i \in I$. Hence $I+(a+bi) = I+(a-8b)$, and the elements of R/I have the form $I+c$ where $0 \le c \le 12$. Therefore, R/I has 13 elements.

4. (1) $1+x+x^3$, $1+x^2+x^3$ (2) $1+x^2$, $2+x+x^2$, $2+2x+x^2$.

These are the polynomials of the relevant degree without a root in the field.

5. (1) If $rs \in p\mathbb{Z}$ then $p \mid rs$ so $p \mid r$ or $p \mid s$ and $r \in p\mathbb{Z}$ or $s \in p\mathbb{Z}$. Also, $p\mathbb{Z} \neq \mathbb{Z}$.

(2) R/I is an integral domain$\Leftrightarrow$ $(I+r)(I+s) = I$ implies that $I+r = I$ or $I+s = I \Leftrightarrow I+rs = I$ implies that $I+r = I$ or $I+s = I \Leftrightarrow rs \in I$ implies that $I+r = I$ or $I+s = I \Leftrightarrow rs \in I$ implies that $r \in I$ or $s \in I \Leftrightarrow$ the ideal I is a prime ideal. (We should note, also, that $I+0 \neq I+1 \Leftrightarrow I \neq R$.)